Міністерство освіти і науки України
Харківський національний університет радіоелектроніки

Факультет _____Комп'ютерної інженерії та управління_____
(повна назва)
Кафедра _____Безпеки інформаційних технологій_____
(повна назва)

АТЕСТАЦІЙНА РОБОТА
Пояснювальна записка

рівень вищої освіти _____другий (магістерський)_____
(рівень вищої освіти)

_____Адміністрування та захист систем на базі ядра Linux_____.
(тема)

Виконав: студент 2 курсу, групи БІКСм-19-1
_____Міщеряков А.Ю._____
(прізвище, ініціали)
Спеціальність 125 Кібербезпека
(код і повна назва спеціальності)
Тип програми _освітньо-професійна_____
(освітньо-професійна або освітньо-наукова)
Освітня програма «Безпека інформаційних і комунікаційних систем»
(повна назва освітньої програми)

Керівник _____проф. Халімов Г.З._____
(посада, прізвище, ініціали)

Допускається до захисту

Зав. кафедри _____ ____Халімов Г.З.____
(підпис) (прізвище, ініціали)

2020 р.

Харківський національний університет радіоелектроніки

Факультет_____Комп'ютерної інженерії та управління_____

Кафедра_____Безпеки інформаційних технологій _____

Рівень вищої освіти_____другий (магістерський)_____

Спеціальність _____125_Кібербезпека_____

Тип програми _____освітньо-професійна_____
(освітньо-професійна, або освітньо-наукова)

Освітня програма_____«Безпека інформаційних і комунікаційних систем»____
(повна назва)

ЗАТВЕРДЖУЮ:
Зав. кафедри _____
(підпис)
«____»_____ 20 ___ р.

ЗАВДАННЯ

НА АТЕСТАЦІЙНУ РОБОТУ

студентові_____Міщерякову Антону Юрійовичу_____
(прізвище, ім'я, по батькові)

1. Тема роботи __Адміністрування та захист систем на базі ядра Linux_____
_____
_____
затверджена наказом по університету від _22_ _____10_____2020 р. № ___1412Ст__
2. Термін подання студентом роботи до екзаменаційної комісії _16_ _____12___ 2020 р.
3. Вихідні дані до роботи _Операційна система Kali Linux та операційна система CentOS_____
_____
_____
4. Перелік питань, що потрібно опрацювати в роботі Безпека збереження паролів в системі та безпечне з'єднання ssh в мережі. Захист системи від вторгнення, та від атаки DDoS на веб-сервер apache
_____
_____
_____
_____
_____
_____

5. Перелік графічного матеріалу із зазначенням креслеників, схем, плакатів, комп'ютерних ілюстрацій (слайдів) _____

6. Консультанти розділів роботи (п.6 включається до завдання за наявності консультантів згідно з наказом, зазначеним у п.1)

Найменування розділу	Консультант (посада, прізвище, ім'я, по батькові)	Позначка консультанта про виконання розділу	
		підпис	дата

КАЛЕНДАРНИЙ ПЛАН

№	Назва етапів роботи	Терміни виконання етапів	Примітка
	Отримання завдання на атестаційну роботу	04.09.2020	
	Пошук та аналіз літературних джерел	04.09.2020	
	Налаштування віртуальної мережі	22.10-27.10.20	
	Налаштування веб-сервера	28.10-07.11.20	
	Тестування заходів захисту	08.11-23.11.20	
	Оформлення пояснювальної записки	24.11-04.12.20	

Дата видачі завдання __22__ _____09_____2020 р.

Студент _____
(підпис)

Керівник роботи _____ _____проф. Халімов Г.З._____
(підпис) (посада, прізвище, ініціали)

РЕФЕРАТ

Атестаційна робота містить: 76 с., 10 таб., 21 рис., 16 джерел.

ВРАЗЛИВІСТЬ, DOS, DDOS, LINUX, МЕРЕЖА, GOLDENEYE, ОПЕРАЦІЙНА СИСТЕМА, ОС, THC HYDRA, APACHE, FAIL2BAN.

Мета роботи – розробити алгоритм захисту від bruteforce та DoS атак на ОС Linux

Об’єкт дослідження – операційна система Unix.

Предмет дослідження – базові утиліти для оцінки захищеності системи.

Метод дослідження – моделювання атаки на ОС та дослідження змін у роботі системи.

Здійснено моделювання bruteforce та DoS атак на операційну систему Linux за допомогою утиліт операційної системи Kali Linux, таких як THC Hydra, John The Riper, GoldenEye. Побудовано алгоритм дій для захисту системи від атак які були змодельовані. Надані рекомендації до налаштування системи.

РЕФЕРАТ

Аттестационная работа содержит: 76 с., 10 таб., 21 рис., 16 источников.

УЯЗВИМОСТЬ, DOS, DDOS, LINUX, МЕРЕЖА, GOLDENEYE, ОПЕРАЦІЙНА СИСТЕМА, ОС, THC HYDRA, APACHE, FAIL2BAN.

Суть роботи – разработать алгоритм защиты от bruteforce и DoS атак на ОС Linux.

Объект исследования – Операционная система Unix.

Предмет исследования – базовые утилиты для оценки защищенности системы.

Метод исследования – моделирование атаки на ОС и исследование измененний в работе системы.

Проведено модлирование атаки на операционную систему Linux с помощью утилит операцуионной системы Kali Linux, таких как THC Hydra, John The Riperб, GoldenEye. Создан алгоритм действий для защиты системы от атак которые были смоделированы. Приведены рекомендации для настройки системы.

ABSTRACT

Research Report: 76 p., 10 tab., 21 d., 16 source

FASTENING, DOS, DDOS, LINUX, NETWORK, GOLDENEYE, OPERATING SYSTEM, OC, THC HYDRA, APACHE, FAIL2BAN.

The purpose of the work – is to develop an algorithm of protection against bruteforce and DoS attacks on the Linux operating system

The object of the study – is the Unix operating system.

Subject of research - basic tools for assessing the security of the system.

The research method – is the simulation of the attack on the OS and the study of changes in the system.

A simulation of the attack on the Linux operating system was carried out with the help of Kali Linux operating system utilities, such as THC Hydra, John The Riper, GoldenEye. An algorithm for protecting the system against attacks that were modeled was constructed. Recommendations for system setup are given.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ

ОС – операційна система

DoS – відмова в обслуговуванні

ПЗ – програмне забезпечення

SSH – Secure Shell

IoT – Internet of things

ВСТУП

На сьогоднішній день все більше людей та фірм переходять на Unix подібні системи для службового користування. Стимулом для переходу стала доступність Unix систем, адже за використання, наприклад Windows Server, необхідно платити великі кошти, коли Unix системи такі як Ubuntu або CentOS безкоштовні.

Рівень кіберпреступності росте, це можна побачити якщо подивитися на рівень в 2015 році та сьогодні. Причиною тому є швидке поширення IoT (або розумних) речей. Завдяки ним DDoS атак стало набагато більше, а самі атаки сильно ускладнилися. З IoT речей ботнети більшої потужності. Так на 2015 рік потужність DDoS атак становила 500 Гб/с, а у 2016 вже 800 Гб/с. Щорічно потужність DDoS атак зростає на 23%, та на 2017 рік становила 1.2 Тб/с.

Зростає також і кількість випадків DDoS атак. Більшість опитаних провайдерів щомісячно фіксували більше 50 DDoS атак. На 2016 рік цей показник становив лише 44%, тобто кількість щомісячних атак зросла приблизна на 60 випадків за рік. Більше ніж 10 атак у місяць стикаються 45% приватних, урядових і освітніх організацій.

Виникає питання проблеми забезпечення інформаційної безпеки. Кожна підприємство бажає надійно захистити свою інформацію, тому що її втрата може бути фатальною для цієї компанії. Виникає необхідність в забезпеченні доступності робітників фірми до необхідної інформації.

Для досягнення цієї цілі створюють користувачів або групи користувачів з різними правами доступу, але для правильної функціональності цієї системи необхідно захищене зберігання файлів з усіма користувачами та паролями, а також перегляд аудита для спостереження за системою.

Також необхідно захистити сервера від DDoS атак, бо немає сенсу налаштовувати політики користувачів якщо сервер не буде доступним.

Метою даної роботи є розробка алгоритму захисту від атаки на паролі серверних операційних систем на базі Unix.

Для цього необхідно розробити заходи захисту від локальної втрати паролів та із мережі.

1 ОПЕРАЦІЙНА СИСТЕМА UNIX

1.1 Поняття операційної системи

Операційна система [1] — це базовий комплекс програмного забезпечення, що виконує управління апаратним забезпеченням комп'ютера або віртуальної машини, забезпечує керування обчислювальним процесом і організовує взаємодію з користувачем. Поняття операційної системи передбачає комплекс взаємопов’язаних системних програм, призначенням яких є забезпечення взаємодії користувача з комп’ютером та функціонування інших програм. Операційна система забезпечує взаємодію між апаратним забезпеченням комп’ютера, прикладними програмами і користувачем.

Операційна система складається з ядра операційної системи та базового набору прикладного програмного забезпечення. Ядро — базовий компонент операційної системи, що реалізує інтерфейс між прикладними процесами та обладнанням комп'ютера. Ядро завантажується в оперативну пам'ять комп'ютера і безпосередньо взаємодіє з апаратурою, забезпечуючи керування апаратними засобами (при цьому використовуються драйвери підключеного в систему обладнання), підтримку одночасної роботи багатьох користувачів (багатокористувацький режим), підтримку паралельного виконання багатьох процесів в системі (багатозадачність). Ядро системи — це набір функцій, структур даних та окремих програмних модулів, які завантажуються в пам'ять комп'ютера при завантаженні операційної системи та забезпечують три типи системних сервісів:

- управління введенням-виведенням інформації (підсистема вводу-виводу ядра ОС);
- управління оперативною пам'яттю (підсистема управління оперативною пам'яттю ядра ОС);
- управління процесами (підсистема управління процесами ядра ОС);

Відносно свого призначення, операційні системи бувають:

- універсальні (для загального використання);
- спеціальні (для розв'язання спеціальних задач);
- спеціалізовані (виконуються на спеціальному обладнанні);
- однозадачні (в окремий момент часу можуть виконувати лише одну задачу);
- багатозадачні (в окремий момент часу здатні виконувати більше однієї задачі);
- однокористувацькі (в системі відсутні механізми обмеження доступу до файлів та на використання ресурсів системи);
- багатокористувацькі (декілька користувачів одночасно і незалежно працюють із операційною системою), всі багатокористувацькі операційні системи також є багатозадачними;
- реального часу (система підтримує механізми виконання задач реального часу, тобто такі, для яких будь які операції завжди виконуються за наперед передбачуваний і незмінний при наступних виконаннях час).

Відносно можливостей внесення змін до вихідного коду операційні системи бувають:

- відкриті— з відкритим програмним кодом;
- комерційні ОС які переважно мають закритий код;

1.2 Атаки на рівні ОС

В загальному випадку програмне забезпечення будь-якої універсальної комп’ютерної системи складається з трьох основних компонентів: операційної системи, мереженого програмного забезпечення і системи управління базами даних. Тому і методи зламу захисту КС можна поділити на 3 групи:

- атаки на рівні операційних систем;
- атаки на рівні мереженого програмного забезпечення;
- атаки на рівня систем керування базами даних.

Внутрішня структура сучасних операційних систем є надзвичайно складною, і тому дотримання адекватної політики безпеки є досить складною задачею.

Успіх реалізації того чи іншого алгоритму хакерської атаки на практиці в значній мірі залежить від архітектури і конфігурації конкретної ОС, яка є об'єктом цієї атаки. Однак, існують атаки, яким може підлягати практично будь-яка операційна система.

Крадіжка пароля:

– підглядання за користувачем, коли той вводить пароль, що дає право на роботу з ОС (навіть якщо під час його введення пароль не висвітлюється на екрані, хакер може легко дізнатись про нього, просто спостерігаючи за переміщенням пальців користувача по клавіатурі);

– отримання пароля з файлу, в якому цей пароль було збережено користувачем, який не бажає утруднювати себе введенням паролю при підключенні до мережі (як правило, такий пароль зберігається у файлі навіть у незашифрованому вигляді);

– пошук пароля, який користувач, щоб не забути його, записує на календарях, в записниках або на зворотній стороні клавіатури (особливо часто таке трапляється, коли адміністратори заставляють користувачів застосовувати паролі, що тяжко запам'ятати);

– крадіжка зовнішнього носія парольної інформації (дискети, електронного ключа, на яких зберігається пароль користувача, призначений для входу в систему);

– повний перебір всіх можливих варіантів паролю;

– підбір пароля за частотою зустрічаємих символів та бітів, за допомогою словників найуживаніших паролів, із залученням знань про конкретного користувача – його імені, прізвища, номера телефону, дати народження, тощо.

Сканування жорстких дисків комп'ютера, коли хакер намагається послідовно звернутись до кожного файлу. Якщо об'єм диска досить великий, то можна бути впевненим, що при описі доступу до файлів і каталогів адміністратор

припустив хоча б одну помилку, в результаті чого, всі такі каталоги і файли будуть прочитані хакером. Для знищення слідів хакер може організувати цю атаку під чужим іменем.

Збирання “сміття” – якщо засоби ОС дозволяють відновлювати раніше знищені об’єкти. Тоді хакер може використати цю можливість щоб отримати доступ до об’єктів, знищених іншими користувачами.

Перевищення повноважень – використовуючи помилки в програмному забезпеченні або в адмініструванні ОС, хакер отримує повноваження, що перевищують надані йому згідно діючій політиці безпеки:

– запуск програм від імені користувача, що має ці необхідні повноваження, або в якості системної програми;

– підміна динамічно завантаженої бібліотеки. що використовується системними програмами, або надання інших значень змінним середовища, що описують шлях до таких бібліотек;

– модифікація коду або даних підсистеми захисту самої операційної системи.

Відмова в обслуговуванні (DoS). Метою цієї атаки є часткове або повне виведення з ладу операційної системи:

– захоплення ресурсів (хакерська програма здійснює захоплення всіх наявних в ОС ресурсів, а потім входить в нескінчений цикл);

– бомбардування запитами (хакерська програма постійно направляє операційній системі запити, реакція на які потребує залучення значних ресурсів комп’ютера);

– використання помилок в програмному забезпеченні або адмініструванні.

1.3 Операційна система Linux

Linux [1]– це операційна система, яка створена на основі загальновідомої системи Unix. Якщо Unix має більше, як 30-літню історію, то датою народження

Linux є 1991 рік. Саме цього року фінський студент Лінус Торвальдс написав невелику системну програму, що дозволяла лише керувати процесами та основною пам’яттю комп’ютера, і звернувся до всіх програмістів із закликом продовжити його роботу. Зусиллями багатьох ентузіастів зі всього світу вже через декілька місяців була створена закінчена операційна система сімейства Unix. Сьогодні Linux стоїть в одному ряду з найпотужнішими операційними системами і продовжує далі розвиватись і розширювати свої функціональні можливості. Жодна серйозна фірма програмного профілю не може ігнорувати цю операційну систему і тому більшість програмних пакетів мають свої версії і для Linux.

Linux функціонує практично на всіх апаратних платформах і підтримує більше типів процесорів і програмних систем, ніж будь-яка інша операційна система. Linux однаково добре працює як на персональних комп’ютерах, так і в комп’ютерних мережах. Її висока мобільність обумовлена як спадковістю від Unix, так і завдячуючи широкій підтримці багатьох програмістів. Linux має повну реалізацію мережного інтерфейсу TCP/IP, що забезпечує підключення до Internet та надання повного спектра послуг цієї всесвітньої мережі.

Linux не тільки багатозадачна операційна система, але це також і система для багатьох користувачів. Навіть на одному комп’ютері можна працювати одночасно на шести текстових консолях і одній графічній.

Варто відзначити дві характерні особливості Linux: безкоштовність та відкритість програмного коду.

Більша частина програмного забезпечення для Linux розроблена в рамках проекту GNU фонду FSF (Free Software Foundation – вільного програмного забезпечення), тому ця операційна система може вільно розповсюджуватись. На відміну від ліцензій для комерційних продуктів, ліцензія GPL (GNU Generic Program License) для Linux захищає авторські права всіх розробників вимагаючи одночасно від них, щоб їх програми і початкові програмні коди були загальнодоступними. Відкритість програмного коду дає також унікальну можливість для самостійного вивчення нових тенденцій в сучасному системному

програмуванні. Саме тому Linux є найкращою базою для використання в навчальному процесі.

Будь-який програміст може написати свою власну програму або внести зміни в існуючі програми, що входять до складу Linux. Звичайно, новостворені програми не завжди проходять жорстке багатомісячне тестування, як це відбувається із новими продуктами відомих фірм. Однак практика підтверджує достатньо високу надійність Linux.

Необхідно розрізняти поняття операційної системи (ОС) і дистрибутиву. ОС – це набір системних програм, призначених, по-перше, для керування ресурсами комп'ютера чи комп'ютерної мережі, по-друге, для полегшення взаємодії користувача з комп'ютером на основі дружнього інтерфейсу. Дистрибутив включає в себе ОС, а також великий набір службових, навчальних, ігрових та інших сервісних програм, зокрема компілятори різних мов програмування, текстові та графічні редактори тощо. Оскільки можна створити різні поєднання ОС із вказаними програмами, тому існує багато різних дистрибутивів. Найбільш відомі із них: Red Hat, Mandrake, Debian, ASP, LFS.

1.4 Опис операційної системи Kali Linux

1.4.1 Історія розвитку Kali Linux

Kali Linux була розроблена фірмой Offensive Security. Вона створена на основі Debian і містить в собі напрацювання дистрибутива для цифрової криміналістики і тестування безпеки BackTrack.

Перша версія BackTrack вийшла в 2006 році, вона об'єднала в собі кілька проектів, основним призначенням яких було тестування на проникнення. Дистрибутив призначався для використання в якості LiveCD.

У 2012 році такий дистрибутив, як BackTrack припинив існувати, а замість нього з'явився Kali Linux, який перейняв всі плюси попередньої версії і все програмне забезпечення. Він був результатом злиття двох проектів: WHAX і Auditor Security Collection. Зараз дистрибутив стабільно розвивається і сили

розробників спрямовані на виправлення помилок та розширення набору інструментів.

1.4.2 Особливості Kali Linux

Kali Linux має спеціалізований проект, відведений для утворення сумісності та перенесення для конкретних пристроїв Android, що називається Kali Linux NetHunter[5].

BackTrack (попередник Kali) мав у собі режим, відомий як forensic mode, який був пізніше перенесений у Kali Linux з live boot. Цей режим дуже популярний, особливо через те, що користувачі мають уже носій із завантажувальною Kali, і цей режим дозволяє легко виконувати криміналістичну роботу. При завантаженні в forensic mode, система не зачіпає внутрішній жорсткий диск і автоматичне встановлення відключене. Проте, розробники рекомендують користувачам перевірити функції перед широким використанням Kali для реальної цифрової криміналістики.

Калі Linux включає в себе багато добре відомих інструментів безпеки, у тому числі Nmap, Aircrack-ng, Kismet, Wireshark, Metasploit, Framework, Burp su te, John the Ripper, Social Engineering Toolkit, Maltego, Ettercap, OWASP ZAP.

Kali Linux поширюється у вигляді 32-розрядних і 64-розрядних образів для використання у вузлах на основі системи команд архітектури x86 і як образ для архітектури ARMдля використання на комп'ютерах BeagleBoard і на Samsung Chromebook.

Розробники Kali Linux ставлять за мету зробити операційну систему доступною для пристроїв на ARM.

Kali Linux доступна для BeagleBone Black, HP Chromebook, CubieBoard 2, CuBox, CuBox-i, Raspberry Pi, EfikaMX, Odroid U2, Odroid XU, Odroid XU3, Samsung Chromebook, Utilite Pro, Galaxy Note 10.1, і SS808.

З приходом Калі NetHunter, Kali Linux теж офіційно доступна на смартфонах, таких як Nexus 5, Nexus 6, Nexus 7, Nexus 9, Nexus 10, OnePlus One, та деяких моделях Samsung Galaxy.

1.4.3 Системні вимоги Kali Linux

Для нормального функціонування Kali Linux необхідно:

– Не менш 20 Гб простору на жорсткому диску.
– Мінімум 1 Гб оперативної пам’яті.
– Завантажувальну флеш носій.

1.4.4 Призначення Kali Linux

Дистрибутив містить безліч інструментів, пов'язаних з безпекою і мережами, які орієнтовані на експертів у комп'ютерній безпеці[5].

Дистрибутив Linux - це не більше ніж ядро і набір базових утиліт, програм і налаштувань за замовчуванням. Kali Linux не надає нічого унікального в цьому плані. Більшість програм може бути просто встановлено в будь-якому іншому дистрибутиві, або навіть в Windows.

Відмінність Kali Linux в тому, що він наповнений такими інструментами і настройками, які потрібні для тестування безпеки, а не для забезпечення нормальної роботи звичайного користувача. Отже, можливості Kali Linux зосереджені на тестуванні безпеки, як це видно з назви.

Особливість Kali Linux в тому що користувач за замовчуванням – root. Це необхідно, тому що багатьом програмам для роботи потрібні права суперкористувача. Це одна з причин, чому не варто використовувати Kali для вирішення повсякденних завдань, наприклад, серфінгу в інтернеті або використання офісних додатків.

1.4.5 Основні утіліти дистрибутива Kali Linux

JHON THE RIPPER

Jhon The Ripper - це інструмент з відкритим вихідним кодом для злому паролів методом перебору. Спочатку він був розроблений для Unix, але зараз доступний на всіх Unix подібних платформах, в тому числі і Linux. Програма також відома як JTR або Jhon. Вона найбільш часто використовується для перебору паролів по словнику[9].

Програма бере текстовий рядок з файлу, шифрує його таким же чином, як був зашифрований пароль, а потім порівнює зашифрований пароль і отриманий

рядок. Якщо рядки співпадають, ви отримуєте пароль, якщо немає, програма бере інший рядок з текстового файлу (словника).

AIRCRACK-NG

Це набір програм для злому і тестування безпеки wifi мереж. Утиліта Aircrack-ng дозволяють зламувати ключі WEP, виконувати моніторинг трафіку, перебирати ключі WPA-PSK, і захоплювати ключі установки з'єднання Wifi. Утиліта Aircrack-ng - це інструменти Kali Linux 2.0, яка використовується найчастіше.

Утиліта дозволяє здійснювати FMS атаки, з деякими оптимізаціями, наприклад, KoreK або PTW, що робить їх більш потужними. Ви можете зламати WEP за кілька хвилин або спробувати перебрати ключ до WPA.

THC HYDRA

THC Hydra - це програмне забезпечення для злому аутентифікації за допомогою перебору. Програма дозволяє виконувати атаки перебору по словнику на більш ніж 50 протоколів, серед яких Telnet, FTP, HTTP, HTTPS, SMB, SSH, VNC, бази даних і багато інших. По суті це простий і швидкий інструмент Kali Linux для злому входу[10].

BURP SUITE

Burp Suite - це інструмент для пошуку вразливостей на сайтах інтернету і в веб-додатках, який може працювати як по HTTP, так і по HTTPS. Він використовується багатьма фахівцями для пошуку помилок і тестування веб-додатків на проникнення. Програма дозволяє об'єднати ручні методи зі своїми засобами автоматизації, щоб виконати тестування якомога ефективніше.

WIRESHARK

Wireshark - це дуже популярний аналізатор мережевих пакетів з відкритим вихідним кодом. Його можна використовувати для усунення неполадок роботи мережі, аналізу додатків і протоколів зв'язку, а також розробки програм.

Програма дозволяє подивитися які пакети проходять через мережевий інтерфейс в реальному часі, надаючи інформація в зручній для сприйняття

формі. Для точного пошуку ви можете використовувати потужну систему фільтрів.

OWASP ZED

Це дуже ефективний інструмент для тестування веб-додатків як для початківців користувачів, так і для професіоналів. Програма дозволяє знаходити уразливості в веб-додатках, тут є автоматизовані сканери, а також різні інструменти, що дозволяють виконувати всю роботу вручну.

METASPLOIT

Metasploit - це дуже популярна платформа для тестування безпеки систем і злому. Можна сказати, що це колекція експлойтів і інструментів, які можуть бути використані для експлуатування різних вразливостей. Програма вийшла в 2004 році і відразу завоювала величезну популярність.

Це найпотужніша платформа для розробки, тестування та використання коду експлойтів. Вона містить інструменти, які дозволяють об'єднати роботу різних компонентів.

ACUNETIX

Це дуже потужний інструмент для сканування веб-сайтів на предмет вразливостей. Сканер Acunetix дозволяє перевірити всі сторінки сайту і виявити можливі SQL-ін'єкції, XSS, XXE, SSRF, атаку на заголовок, і інші 3000 відомих вразливостей.

NMAP

Namp або Network Mapper - це утиліта Kali Linux з відкритим вихідним кодом, яка може використовуватися для аудита безпеки мереж і сканування портів. Безліч адміністраторів використовують Nmap для перегляду пристроїв, підключених до локальної мережі, перевірки відкритих портів або моніторингу безперебійної роботи серверів.

За допомогою Nmap будь-який користувач може визначити чи доступні його локальні програми з мережі.

CAIN AND ABEL

Cain and Abel або просто Cain це дуже популярний інструмент для перебору паролів. Спочатку він призначався для відновлення пароля Microsoft Windows, але він може використовуватися для інших цілей.

Для отримання паролів можна використовувати перехоплення пакетів, перебір хеш, атаки по словнику, аналіз райдужних таблиць і атаки криптоаналізу.

NIKTO WEBSITE VULNERABILITY SCANNER

Це ще один класичний інструмент для сканування серверів на наявність вразливостей. Програма проводить пошук по базі більше 6000 потенційно небезпечних файлів, також може виявляти застарілі версії мережевого програмного забезпечення для понад 1300 різних програм, також ви можете перевірити конфігураційні файли сервера.

SOCIAL-ENGINEER TOOLKIT

Social-Engineer Toolkit - це інструмент, який дозволяє виконувати різні атаки соціального інжинірингу. Ця програма на Python дозволяє виконувати різні соціальні атаки, автоматизувати виконання атак, генерувати повідомлення електронної пошти, маскувати шкідливі веб-сторінки і багато іншого.

1.5 Статистика уразливостей Linux

Linux Kernel - ядро операційної системи, основа ОС сімейства Linux. Іншими словами, це нутрощі ОС, тоді як зовнішня оболонка може бути різною. Перша поява - 1991 рік. Незважаючи на велику кількість вразливостей, виявлених за період з 1999 по 2017 рік, ОС Linux не так популярна серед кіберзлочинців. А все пов'язано з її малим поширенням в світі. За деякими даними всього 1% від загального числа користувачів комп'ютерів використовують саме цю ОС. А для отримання більшого профіту зловмисникам потрібно більше жертв[8]. Графік уразливостей за 2017 рік можна побачити на рисунку 1.1.

Рисунок 1.1 – Графік уразливостей ОС Linux

1.5.1 Уразливості категорії “DoS”

Уразливість 1

Функція inet_csk_clone_lock в net / ipv4 / inet_connection_sock.c дозволяє зловмисникам організувати DoS за допомогою управління прийнятим системним викликом.

Уразливість 2

Функція mq_notify в ядрі Linux не встановлює значення покажчика сокета на NULL при вході в режим повторів. Під час закриття сокета Netlink призначеним для користувача простором, зловмисники можуть організувати DoS.

Netlink - інтерфейс ядра Linux для установки зв'язку між призначеними для користувача процесами і процесами самого ядра.

Уразливість 3

Функція __skb_flow_dissect в net / core / flow_dissector.c не посвідчується в тому, що n_proto, ip_proto і thoff ініціалізовані, що дозволяє влаштувати DoS або виконати довільний код через створений MPLS пакет.

Додаткова інформація по уразливостям наведена в таблиці 1.1.

Таблиця 1.1. – Уразлиості категорії DoS.

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп види уразливостей
			Конфіденційність	Цілісність	Доступність		
1	2017-8890	10/05/2017	Повний	Повний	Повний	Не потрібна	-
2	2017-11176	11/07/2017	Повний	Повний	Повний	Не потрібна	-
3	2017-13715	26/08/2017	Повний	Повний	Повний	Не потрібна	Виконання коду

1.5.2 Уразливісті категорії “Обходу”

Уразливість 1

Програмне переповнення призводить до стану TOCTOU в гіпервізора PIL (Peripheral Image Loader), також викликає стан гонки, що може бути використано для обходу аутентифікації в PIL.

TOCTOU - Time of check to time of use - клас багів, викликаних змінами в системі між перевіркою стану (наприклад, облікові дані входу) і використанням результатів цієї перевірки.

Стан гонки - помилка проектування багатопотокової системи або додатки, коли робота системи або додатки залежить від порядку виконання коду.

Уразливість 2

arch/arm64/kernel/sys.c в ядрі Linux до версії 4.0 дозволяло користувачам обійти захисний механізм «strict page permissions» і модифікувати таблицю системних викликів, надалі отримуючи привцлеї, експлуатуючи доступ до запису.

Уразливість 3

Уразливість розкриття інформації в засобі завантаження Qualcomm може дати локальному шкідливому ПО виконати довільний код у контексті завантажувача.

Додаткова інформація по уразливостям наведена в таблиці 1.2.

Таблиця 1.2 – Уразливості категорії обходу чого-небудь

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп. види уразливостей
			Конфіденційність	Цілісність	Доступність		
1	2016-8438	12/01/2017	Повний	Повний	Повний	Не потрібна	Переповнення
2	2015-8967	08/12/2015	Повний	Повний	Повний	Не потрібна	Здобуття привілеїв
3	2017-0455	07/03/2017	Повний	Повний	Повний	Не потрібна	Виконання коду

1.5.3 Уразливість категорії “Виконання коду”

Уразливість 1

udp.c в ядрі Linux версій до 4.5 дозволяє віддалено виконати довільний код через UDP трафік, який запускає небезпечне обчислення другої контрольної суми під час виконання системного виклику recv з прапором MSG_PEEK.

Уразливість 2

Уразливість в прошивці Broadcom Wi-Fi давала можливість віддалено виконати довільний код всередині контексту Wi-Fi SoC.

Уразливість 3

Функція __skb_flow_dissect в net / core / flow_dissector.c не посвідчується в тому, що n_proto, ip_proto і thoff ініціалізовані, що дозволяє влаштувати DoS або виконати довільний код через створений MPLS пакет.

Додаткова інформація по уразливостям наведена в таблиці 1.3.

Таблиця 1.3 – Уразливість категорії виконання коду

Уразливість(№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп. види уразливостей
			Конфіденційність	Цілісність	Доступність		
1	2016-10229	04/04/2017	Повний	Повний	Повний	Не потрібна	-
2	2017-0561	07/04/2017	Повний	Повний	Повний	Не потрібна	-
3	2017-13715	28/08/2017	Повний	Повний	Повний	Не потрібна	DoS

1.5.4 Уразливості катергорії “Пошкодження пам'яті”

Уразливість 1

Переповнення буфера в RNDIS імплементації USB давало можливість влаштувати DoS через віддалений NDIS відгук до OID_GEN_SUPPORTED_LIST, що призводило до виділення пам'яті на дані відповіді, а не на його структуру.

Уразливість 2

Програмна помилка в функції CIFSFindNext в fs / cifs / cifssmb.c дозволяла віддалених серверів CIFS створювати DoS через велике значення довжини у відповіді на запит читання директорії.

Уразливість 3

sound / soc / msm / qdsp6v2 / msm-audio-effects-q6-v2.c в звуковому драйвері MSM QDSP6 для ядра Linux 3.x, використовуваного в MSM пристроях на базі Android від Qualcomm Innovation Center (QuIC), давало можливість організувати DoS через створене додаток, яке змушувало ioctl викликати неправильне використання покажчика параметрів.

ioctl - системний виклик для операцій введення-виведення та інших, які не можуть бути оброблені звичайними системними викликами.

Додаткова інформація по уразливостям наведена в таблиці 1.4.

Таблиця 1.4 – Уразливості категорії “Пошкодження пам’яті”

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп. види уразливостей
			Конфіденційність	Цілісність	Доступність		
1	2006-1368	23/03/2006	Повний	Повний	Повний	Не потрібна	DoS, переповнення
2	2011-3191	24/05/2012	Повний	Повний	Повний	Не потрібна	DoS
3	2016-2065	07/08/2016	Повний	Повний	Повний	Не потрібна	DoS

1.5.5 Уразливості категорії “Доступ до інформації”

Уразливість 1

Уразливість розкриття інформації в засобі завантаження Qualcomm може дати локальному шкідливому ПО виконати довільний код у контексті завантажувача.

Уразливість 2

OZWPAN драйвер спирається на ненадійний атрибут під час парсинга пакетів, що дозволяє провести DoS і отримати доступ до цінної інформації з пам'яті ядра за рахунок створеного пакета.

Уразливість 3

Імплементація xfs в ядрі до версії 2.6.35 не проглядається btrees структуру inode-ів перед читанням буферів inode-ів, що дозволяє віддаленому аутентифікованим користувачеві зчитувати незв'язані файли, або зчитувати і перезаписувати дискові блоки, які на момент операції підв'язані до активного

файлу, але раніше були підв'язані до непов'язаній файлу, шляхом доступу до NFS.

– inode (індексний дескриптор) - структура даних
– btrees - структура даних, дерево пошуку
– NFS - протокол мережевого доступу до файлових систем

Додаткова інформація по уразливостям наведена в таблиці 1.5.

Таблиця 1.5 – Уразливості категорії “доступ до інформації”

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп. види уразливостей
			Конфіденційність	Цілісність	Доступність		
1	2017-0455	07/03/2017	Повний	Повний	Повний	Не потрібна	Виконання коду, обхід обмежень
2	2015-4004	07/06/2015	Частичний	Нульовий	Повний	Не потрібна	DoS, переповнення
3	2010-2943	30/09/2010	Повний	Повний	Single system	Не потрібна	

1.5.6 Уразливості категорії “збільшення привілеїв”

Уразливість 1

Функція «capabilities» (можливості) в Linux до версії 2.2.16 дозволяла локальним користувачам отримати привілеї шляхом настройки capabilities для запобігання зняття привілеїв setuid программой.

setuid - установка ID користувача під час виконання

Уразливість 2

Множинне програмне переповнення в 32-бітному емуляторі для AMD64 архітектур дозволяв зловмисникам провести DoS або отримати привілеї рута через невстановлені вектори, які активували функціональні виклики copy_from_user з неправильними аргументами довжини.

Mnozhynne prohramne perepovnennya v 32-bitnomu emulyatori dl

Уразливість 3

Уразливість Use-after-free в функції kvm_ioctl_create_device в virt / kvm / kvm_main.c дозволяла користувачу-хосту проводити DoS або отримати привілеї через створені ioctl виклики на / dev / kvm пристрій.

Додаткова інформація по уразливостям наведена в таблиці 1.6.

Таблиця 1.6 – Уразливості категорії “збільшення привілеїв”

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп види уразливості
			Конфіденційність	Цілісність	Доступність		
1	2000-0506	09/06/2000	Повний	Повний	Повний	Не потрібна	DoS
2	2003-0959	31/12/2003	Повний	Повний	Повний	Не потрібна	DoS, переповнення
3	2016-10150	06/02/2017	Повний	Повний	Повний	Не потрібна	DoS

1.5.7 Уразливість категорії “переповнення”

Уразливість 1

Можливе програмне переповнення в системному виклику SMMU. Невірна помилки під час введення в системному виклику ADSP SID2CB може привести до перезапису пам'яті гіпервізора.

Уразливість 2

Переповнення буфера в підсистемі сховища. Неправильні як частина відповіді до RPMB командам може привести до переповнення буфера.

Уразливість 3

/drivers/isdn/i4l/isdn_net.c: буфер, контрольований користувачем, копіюється в локальний буфер в константному розмірі з використанням strcpy без перевірки довжини, що може привести до переповнення буфера.

Додаткова інформація по уразливостям наведена в таблиці 1.7.

Таблиця 1.7 – Уразливості категорії “переповнення”

Уразливість (№)	Код по CVE	Дата	Рівень впливу на			Автентифікація	Доп види уразливості
			Конфіденційність	Цілцстність	Доступність		
1	2000-0506	09/06/2000	Повний	Повний	Повний	Не потрібна	DoS
2	2003-0959	31/12/2003	Повний	Повний	Повний	Не потрібна	DoS, переповнення
3	2016-10150	06/02/2017	Повний	Повний	Повний	Не потрібна	DoS

2 DOS ТА DDOS АТАКИ

DoS (від англ. Denial of Service «відмова в обслуговуванні») - хакерська атака на обчислювальну систему з метою довести її до відмови, тобто створення таких умов, при яких сумлінні користувачі системи не зможуть отримати доступ до надаваних системних ресурсів (серверів), або цей доступ буде утруднений. Відмова «ворожої» системи може бути і кроком до оволодіння системою (якщо в нештатної ситуації ПО видає будь-яку критичну інформацію - наприклад, версію, частина програмного коду і т. д.). Але частіше це міра економічного тиску: втрата простий служби, що приносить дохід, рахунки від провайдера і заходи по догляду від атаки відчутно б'ють «мета» по кишені. В даний час DoS і DDoS-атаки найбільш популярні, так як дозволяють довести до відмови практично будь-яку систему, не залишаючи юридично значимих доказів.

2.1 Розподілена DoS-атака

Якщо атака виконується одночасно з великої кількості комп'ютерів, говорять про DDoS-атаці (від англ. Distributed Denial of Service, розподілена атака типу «відмова в обслуговуванні»). Така атака проводиться в тому випадку, якщо потрібно викликати відмову в обслуговуванні добре захищеною великої компанії або урядової організації.

Насамперед зловмисник сканує велику мережу за допомогою спеціально підготовлених сценаріїв, які виявляють потенційно слабкі вузли. Обрані вузли піддаються нападу, і зловмисник отримує на них права адміністратора. На захоплені вузли встановлюються троянські програми, які працюють у фоновому режимі. Тепер ці комп'ютери називаються комп'ютерами-зомбі, їх користувачі навіть не підозрюють, що є потенційними учасниками DDoS-атаки. Далі зловмисник відправляє певні команди захопленим комп'ютерів і ті, в свою чергу здійснюють колективну DoS-атаку на цільовий комп'ютер.

Існують також програми для добровільної участі в DDoS-атаках.

У деяких випадках до фактичної DDoS-атаці призводить ненавмисне дію, наприклад, розміщення на популярному інтернет-ресурсі посилання на сайт, розміщений на не дуже продуктивному сервері (слешдот-ефект). Великий наплив користувачів призводить до перевищення допустимого навантаження на сервер і, отже, відмови в обслуговуванні частини з них.

2.1.1 Захист

Для захисту від мережевих атак застосовується ряд фільтрів, підключених до інтернет-каналу з великою пропускною здатністю. Фільтри діють таким чином, що послідовно аналізують проходить трафік, виявляючи нестандартну мережеву активність і помилки. У числі аналізованих шаблонів нестандартного трафіку входять всі відомі на сьогоднішній день методи атак, в тому числі реалізовані і за допомогою розподілених бот-мереж. Фільтри можуть реалізовуватися як на рівні маршрутизаторів, керованих свічів, так і спеціалізованими апаратними засобами. Фахівці в області захисту інформації виділяють кілька причин використання DDoS-атак.

2.1.2 Причини викроистання DDoS-атак

– Особиста неприязнь

Ця причина нерідко є приводом для атак на великі комерційні та урядові організації та компанії. Так в 1999 році були атаковані Web-вузли ФБР, які згодом були недоступні протягом декількох тижнів. Мотивом послужив нещодавній рейд ФБР проти хакерів.

– Розвага

В даний час все більше людей цікавляться DoS-атаками, і всі хочуть спробувати себе в цій справі. Тому багато початківці зловмисники здійснюють DoS-атаки заради розваги. Після успішно проведеного нападу вони дивляться масштаби своїх руйнувань.

– Політичний протест

Найбільш відомими DDoS-атаками з метою політичного протесту були акції на підтримку Пам'ятника Воїну-визволителю в Естонії (2007), Південної Осетії (2008), Wikileaks (2011), Megaupload (2012) і EX.UA (2012).

– Недобросовісна конкуренція.

– Вимагання або шантаж.

2.1.3 Класифікація DoS-атак

Хакерам набагато легше здійснити DoS-атаку на систему, ніж отримати повний доступ до неї. Існують різні причини, через які може виникнути DoS-умова, тобто така ситуація, при якій користувачі не можуть отримати доступ до ресурсів, які надає сервер, або доступ до них ускладнений:

– Насичення смуги пропускання

В даний час практично кожен комп'ютер підключений до мережі Internet або до локальної мережі. Це служить відмінним приводом для здійснення DoS-атаки за рахунок переповнення смуги пропускання. Зазвичай зловмисники користуються флудом (англ. Flood - «повінь», «переповнення») - атака, пов'язана з великою кількістю зазвичай безглуздих або сформованих в неправильному форматі запитів до комп'ютерної системи або мережевого обладнання, що має своєю метою або яка призвела до відмови в роботі системи з -за вичерпання системних ресурсів - процесора, пам'яті або каналів зв'язку. Є кілька різновидів флуду.

– HTTP-флуд і ping-флуд

Це найпримітивніший вид DoS-атаки. Насичення смуги пропускання можна здійснити за допомогою звичайних ping-запитів тільки в тому випадку, якщо канал атакуючого набагато ширше каналу комп'ютера-жертви. Але така атака марна проти сервера, так як той, в свою чергу, має досить широкою смугою пропускання. Для атаки на сервер зазвичай застосовується HTTP-флуд. Атакуючий шле маленький за обсягом HTTP-пакет, але такий, щоб сервер відповів на нього пакетом, розмір якого в сотні разів більше. Навіть якщо канал сервера в десять разів ширше каналу атакуючого, то все одно є великий шанс

наситити смугу пропускання жертви. А для того, щоб відповідні HTTP-пакети не викликали відмову в обслуговуванні у зловмисника, він кожен раз підміняє свій ip-адреса на ip-адреси вузлів в мережі.

– Smurf-атака (ICMP-флуд)

Атака Smurf або ICMP-флуд - один з найнебезпечніших видів DoS-атак, так як у комп'ютера-жертви після такої атаки відбудеться відмова в обслуговуванні практично з 100% гарантією. Зловмисник використовує трансляцію розсилку для перевірки працюючих вузлів в системі, відправляючи ping-запит. Очевидно, атакуючий поодинці не зможе вивести з ладу комп'ютер-жертву, тому потрібно ще один учасник - це підсилює мережу. У ній по широкомовною адресою зловмисник відправляє підроблений ICMP пакет. Потім адресу атакуючого змінюється на адресу жертви. Всі вузли надішлють їй відповідь на ping-запит. Тому ICMP-пакет, відправлений зловмисником через посилює мережу, що містить 200 вузлів, буде посилено в 200 разів. Для такої атаки зазвичай вибирається велика мережа, щоб у комп'ютера-жертви не було ніяких шансів.

– Атака Fraggle (UDP-флуд)

Атака Fraggle (осколкова граната) (від англ. Fraggle attack) є повним аналогом Smurf-атаки, де замість ICMP пакетів використовуються пакети UDP, тому її ще називають UDP-флуд. Принцип дії цієї атаки простий: на сьомий порт жертви відправляються echo-команди по широкомовному запиту. Потім підміняється ip-адреса зловмисника на ip-адресу жертви, яка незабаром отримує безліч повідомлень-відповідей на них. Їх кількість залежить від числа вузлів в мережі. Ця атака призводить до насичення смуги пропускання і повної відмови в обслуговуванні жертви. При цьому, якщо служба echo відключена, то будуть згенеровані ICMP-повідомлення, що також призведе до насичення смуги.

– SYN-флуд

До появи атаки Smurf була широко поширена атака за допомогою переповнення пакетами SYN, також відома під назвою SYN-флуд. Для опису її дії можна зупинитися на розгляді двох систем A і B, які хочуть встановити між собою TCP з'єднання, після якого вони зможуть обмінюватися між собою даними. На установку з'єднання виділяється певна кількість ресурсів, цим і користуються DoS-атаки. Відправивши кілька помилкових запитів, можна витратити всі ресурси системи, відведені на встановлення з'єднання. Розглянемо докладніше, як це відбувається. Хакер з системи A відправляє пакет SYN системі B, але попередньо помінявши свій IP-адресу на неіснуючий. Потім, нічого не підозрюючи, комп'ютер B відправляє відповідь SYN / ACK на неіснуючий IP-адреса і переходить в стан SYN-RECEIVED. Так як повідомлення SYN / ACK не дійде до системи A, то комп'ютер У ніколи не отримає пакет з прапором ACK. Дане потенційне з'єднання буде поміщено в чергу. З черги воно вийде тільки після закінчення 75 секунд. Цим користуються зловмисники і відправляють відразу кілька пакетів SYN на комп'ютер жертви з інтервалом в 10 секунд, щоб повністю вичерпати ресурси системи. Визначити джерело нападу дуже непросто, тому що зловмисник постійно змінює вихідний IP-адресу.

– Недолік ресурсів

Зловмисники вдаються до даного виду DoS-атаки для захоплення системних ресурсів, таких як оперативна і фізична пам'ять, процесорний час і інші. Зазвичай такі атаки проводяться з урахуванням того, що хакер вже володіє деякою кількістю ресурсів системи. Метою атаки є захоплення додаткових ресурсів. Для цього не обов'язково насичувати смугу пропускання, а досить просто перевантажити процесор жертви, тобто зайняти все допустиме процесорний час.

– Відправлення «важких» запитів

Атакуючий посилає серверу пакети, що не насичують смугу пропускання (канал зазвичай досить широкий), але витрачають все його процесорний час. Процесор сервера, коли буде їх обробляти, може не впоратися зі складними обчисленнями. Через це станеться збій, і користувачі не зможуть отримати доступ до необхідних ресурсів.

– Переповнення сервера лог-файлами

Лог-файли сервера - це файли, в яких записуються дії користувачів мережі або програми. Некваліфікований адміністратор може неправильно налаштувати систему на своєму сервері, що не встановивши певний ліміт. Хакер скористається цією помилкою і буде відправляти великі за обсягом пакети, які незабаром займуть весь вільний місце на жорсткому диску сервера. Але ця атака спрацює тільки в разі з недосвідченим адміністратором, кваліфіковані зберігають лог-файли на окремому системному диску.

– Погана система квотування

На деяких серверах є так звана CGI-програма, яка пов'язує зовнішню програму з Web-сервером. Якщо хакер отримає доступ до CGI, то він зможе написати скрипт (англ. Scripting language), який задіює чимало ресурсів сервера, таких як оперативна пам'ять і процесорний час. Наприклад, скрипт CGI може містити в собі циклічне створення великих масивів або обчислення складних математичних формул. При цьому центральний процесор може звертатися до такого скрипта кілька тисяч разів. Звідси висновок: якщо система квотування налаштована неправильно, то такий скрипт за малий час відніме всі системні ресурси у сервера. Звичайно, вихід з цієї ситуації очевидний - поставити певний ліміт на доступ до пам'яті, але і в цьому випадку процес скрипта, досягнувши цього ліміту, буде знаходитися в очікуванні до тих пір, поки не вивантажить з пам'яті всі старі дані. Тому користувачі будуть відчувати нестачу в системних ресурсах.

– Недостатня перевірка даних користувача

Недостатня перевірка даних користувача також призводить до нескінченного або тривалого циклу або підвищеному тривалого споживання процесорних ресурсів (аж до вичерпання процесорних ресурсів) або виділення великого обсягу оперативної пам'яті (аж до вичерпання доступної пам'яті).

– Атака другого роду

Це атака, яка прагне викликати помилкове спрацьовування системи захисту і таким чином привести до недоступності ресурсу.

– Помилки програмування

Професійні реалізатори DoS-атак не використовують такий примітивний спосіб атаки, як насичення смуги пропускання. Повністю розібравшись у структурі системи жертви, вони пишуть програми (експлойти), які допомагають атакувати складні системи комерційних підприємств або організацій. Найчастіше це помилки в програмному коді, що призводять до звернення до невикористовуваних фрагменту адресного простору, виконання неприпустимою інструкції або іншої необроблюваної виняткової ситуації, коли відбувається аварійне завершення програми-сервера - серверної програми. Класичним прикладом є звернення за нульовим (англ. Null) адресою.

– Недоліки в програмному коді

Обробка виняткових ситуацій завжди була головним болем для творців операційних систем. Зловмисники шукають помилки в програмному коді будь-якої програми або операційної системи, змушують її обробляти такі виняткові ситуації, які вона обробляти не вміє. За рахунок цього виникають помилки. Простим прикладом може служити часта передача пакетів, в якій не враховуються специфікації і стандарти RFC-документів. Зловмисники спостерігають за тим, чи справляється мережевий стек з обробкою виняткових ситуацій. Якщо немає, то передача таких пакетів призведе до паніки ядра (kernel panic) або навіть до краху всієї системи в цілому.

До цього класу належить помилка Ping of death, поширена в 1990-і роки. Довжина пакета IPv4 за стандартом RFC 791 IPv4 не може перевищувати 65 535

байт; комп'ютера-жертви надсилається ICMP-пакет більшої довжини, попередньо розбитий на частини; у жертви від такого пакета переповнюється буфер. Інша помилка тих часів - WinNuke (Windows 95 неправильно обробляла рідкісний біт TCP-пакета URG).

– Переповнення буфера

Переповнення буфера виникає в тому випадку, якщо програма через помилки програміста записує дані за межами буфера. Припустимо, програміст написав додаток для обміну даними по мережі, яке працює за будь-якою протоколу. У цьому протоколі суворо вказано, що певний поле пакету максимум може містити 65536 байт даних. Але після тестування програми виявилося, що в її клієнтської частини в це поле не потрібно поміщати дані, розмір яких більше 255 байт. Тому і серверна частина прийме не більше 255 байт. Далі зловмисник змінює код програми так, що тепер клієнтська частина відправляє всі допустимі по протоколу 65536 байт, але сервер до їх прийому не готовий. Через це виникає переповнення буфера, і користувачі не можуть отримати доступ до додатка.

2.1.4 Маршрутизація і атаки DNS

Всі атаки на DNS-сервери можна розбити на два типи: DoS-атаки на уразливості в програмному забезпеченні на DNS-серверах та DDoS атаки на DNS-сервери.

– DoS-атаки на уразливості в програмному забезпеченні на DNS-серверах

Їх ще називають атаками на кеш. В процесі цієї атаки зловмисник підміняє IP-адреса DNS-сервера домена жертви. Після чого атакується при запиті HTML-сторінки, потрапляє або в «чорну діру» (якщо IP-адреса був замінений на неіснуючий), або прямо на сервер зловмисника. Другий випадок більш плачевний, так як зловмисник легко може отримати доступ до особистих даних нічого не підозрюючи жертви. Розглянемо на прикладі, як це відбувається. Припустимо, що клієнт хоче потрапити на Web-вузол компанії microsoft.com. Але використавши уразливість в DNS-сервері компанії, зловмисник підмінив IP-

адреса вузла microsoft.com на свій. Тепер жертва автоматично перенаправляється на вузол до атакуючого.

– DDoS атаки на DNS-сервери

Далі мова піде про DDoS-атаках, так як участь DNS-серверів завжди має на увазі наявність великої кількості комп'ютерів. Атаки на DNS-сервери - найбанальніші атаки, що призводять до відмови в обслуговуванні DNS-сервера як шляхом насичення смуги пропускання, так і шляхом захоплення системних ресурсів. Але така атака вимагає величезної кількості комп'ютерів-зомбі. Після її успішного проведення користувачі не можуть потрапити на потрібну їм сторінку в Інтернеті, тому що DNS-сервер не може перетворити доменне ім'я в IP-адресу сайту. Але в даний час атаки на DNS-сервери з використанням великої кількості комп'ютерів-зомбі (таку систему називають «ботнет») менш актуальні, так як інтернет-провайдери легко помічають велика кількість вихідного трафіку і блокують його. Зловмисники тепер обходяться невеликими ботнетами, або не використовують їх зовсім. Основна ідея полягає в тому, що хакери використовують DNS-сервери, що працюють на основі технології DNSSEC. Потужність атаки зростає внаслідок збільшення відображень DNS-запитів. В ідеалі DNS-сервери певного провайдера повинні обробляти тільки ті запити, які прийшли до них від користувачів цього провайдера, але це далеко від реальності. По всьому світу дуже багато некоректно налаштованих серверів, які можуть прийняти запит від будь-якого користувача в Інтернеті. Працівники компанії CloudFlare стверджують, що в даний час в Інтернеті більш 68 тисяч неправильно налаштованих DNS-серверів, з них більше 800 - в Росії. Саме такі DNS-сервери використовуються для DDoS-атак. Основна ідея полягає в тому, що практично всі DNS-запити пересилаються по протоколу UDP, в якому порівняно просто підмінити зворотну адресу на адрес жертви. Тому через неправильно сконфігуровані DNS-сервери зловмисник шле такий запит, щоб відповідь на нього був якомога більше за обсягом (наприклад, це може бути список всіх записів в таблиці DNS), в якому зворотний IP-адреса підміняється на IP-адресу жертви. Як правило, сервери провайдерів мають досить велику пропускну

здатність, тому сформувати атаку в кілька десятків Гбіт / с не складає особливих труднощів.

Таблиця 2.1 Список автономних систем з найбільшим числом неправильно сконфігурованих DNS-серверів

Число DNS-серверів	Ім'я автономної системи
2108	BELPAK-AS Republican Unitary Telecommunication Enterprise Be
1668	HINET Data Communication Business Group
1596	OCN NTT Communications Corporation
1455	TELEFONICA CHILE S.A.
1402	KIXS-AS-KR Korea Telecom
965	Telefonica de Argentina
894	ERX-TANET-ASN1 Tiawan Academic Network (TANet) Information C
827	KDDI KDDI CORPORATION
770	Compa Dominicana de Telefonos, C. por A. — CODETEL
723	CHINANET-BACKBONE No.31,Jin-rong Street
647	LGDACOM LG DACOM Corporation
606	UUNET — MCI Communications Services, Inc. d/b/a Verizon Busi
604	TELKOMNET-AS2-AP PT Telekomunikasi Indonesia
601	COLOMBIA TELECOMUNICACIONES S.A. ESP

2.1.5 Виявлення DoS / DDoS-атак

Існує думка, що спеціальні засоби для виявлення DoS-атак не потрібні, оскільки факт DoS-атаки неможливо не помітити. У багатьох випадках це дійсно так. Однак досить часто спостерігалися вдалі DoS-атаки, які були помічені жертвами лише через 2-3 діб. Бувало, що негативні наслідки атаки (флуд-атаки)

виливалися в зайві витрати на оплату надлишкового Internet-трафіку, що з'ясовувалося лише при отриманні рахунку від Internet-провайдера. Крім того, багато методи виявлення атак неефективні поблизу об'єкта атаки, але ефективні на мережевих магістральних каналах. В такому випадку доцільно ставити системи виявлення саме там, а не чекати, поки користувач, що піддався атаці, сам її помітить і звернеться за допомогою. До того ж для ефективної протидії DoS-атак необхідно знати тип, характер і інші характеристики DoS-атак, а оперативно отримати ці відомості як раз і дозволяють служби забезпечення безпеки. Вони допомагають зробити деякі налаштування системи. Але визначити, чи була дана атака проведена зловмисником, або відмова в обслуговуванні був наслідком нештатного події, вони не можуть. Відповідно до правил політики забезпечення безпеки, при виявленні DoS або DDoS-атаки потрібно її реєстрація для подальшого аудиту. Після того, як атака була зафіксована, можуть знадобитися служби забезпечення безпеки для деяких коригувань у системі і для її повернення до колишнього рівня роботи. Також для виявлення DDoS-атаки можуть використовуватися служби, не пов'язані з безпекою, наприклад, перенаправлення трафіку по інших каналах зв'язку, включення резервних серверів для копіювання інформації. Таким чином, кошти для виявлення і запобігання DDoS-атак можуть сильно відрізнятися в залежності від виду захищається системи.

Методи виявлення DoS-атак можна розділити на кілька великих груп:

– сигнатурні - засновані на якісному аналізі трафіку.

– статистичні - засновані на кількісному аналізі трафіку.

– гібридні (комбіновані) - поєднують в собі переваги обох вищезгаданих методів.

2.1.6 Відомі DDoS-атаки

У 2012 році було проведено кілька великомасштабних DDoS-атак на DNS-сервери. Перша з них планувалася на 31 березня, але так і не відбулася. Метою зловмисників з групи Anonymous було довести до відмови всю глобальну мережу Інтернет. Вони хотіли це зробити за допомогою DDoS-атаки на 13 кореневих

DNS-серверів. Зловмисники випустили спеціальну утиліту Ramp, яка призначалася для об'єднання дрібніших DNS-серверів і інтернет-провайдерів. За допомогою них і планувалося вивести з ладу глобальну мережу.

Точно така ж атака була проведена в листопаді 2002 року. Її досі вважають самої глобальної DDoS-атакою на DNS-сервери, так як в результаті зловмисники змогли вивести з ладу 7 кореневих серверів. Наступна атака пройшла в серпні на компанію AT & T, що є найбільшою американською телекомунікаційною компанією. В результаті після атаки, яка тривала 8 годин, вийшли з ладу DNS-сервери компанії. Користувачі деякий час не могли зайти не тільки на сайт компанії AT & T, але і на комерційні сайти в її мережі.

Ще одна атака відбулася 10 листопада 2012 року на компанію Go Daddy, яка є найбільшим в світі хостинг-провайдером. Наслідки атаки були руйнівні: постраждав не тільки сам домен www.godaddy.com, а й понад 33 мільйонів доменів в мережі Інтернет, які були зареєстровані компанією.

Набагато раніше, 22 серпня 2003 зловмисники за допомогою вірусу Mydoom вивели з ладу сайт компанії SCO, що займається розробкою системного програмного забезпечення. Цілих 3 дні користувачі не могли потрапити на сайт компанії.

15 вересня 2012 року, велика DDoS-атака потужністю в 65 Гбіт / с обрушилася на компанію CloudFlare, яка є мережею доставки контенту, призначена для віртуального хостингу. Сервери даної компанії розташовані по всьому світу. Це допомагає користувачеві завантажувати сторінку в Інтернеті з найближчого (з географічної точки зору) сервера CloudFlare набагато швидше. Раніше дана компанія витримувала DDoS-атаки потужністю в кілька десятків Гбіт / с, але з атакою в 65 Гбіт / с впоратися не змогла. Цей пік припав на суботу 15 вересня в 13.00. Співробітники, які працювали на той момент в компанії CloudFlare, були колишніми хакерами, яким стало цікаво розібратися, яким же саме методом була проведена дана DDoS-атака, і як зловмисники змогли провести її з такою потужністю. Виявилося, що для такої атаки треба було б 65 тисяч ботів, створюють трафік в 1 Мбіт / с кожен. Але це неможливо, так як

інтернет-провайдери з легкістю знайдуть і заблокують такий великий обсяг трафіку. При цьому оренда великого ботнету дуже дорого обходиться. Тому з'ясувалося, що для такої атаки використовувався метод примноження DNS-запитів через відкриті DNS-сервери.

Приблизно через півроку, 18 березня, розпочалася, за версією газети The New York Times, найбільша DDoS-атака в історії, жертвою якої стала компанія Spamhaus, що займається занесенням в чорний список джерел спаму. Причиною атаки послужив той факт, що Spamhaus занесла в чорний список за розсилку спаму голландського хост-провайдера Cyberbunker. Другий своє невдоволення висловив за допомогою DDoS-атаки з піковою потужністю в 300 Гбіт / с через відкриті DNS-сервери. 19 березня потужність досягла 90 Гбіт / с, змінюючи своє значення від 30 Гбіт / с. Після цього було затишшя, але воно тривало недовго і атака відновилася з новою силою і 22 березня її потужність досягла 120 Гбіт / с. Для відбиття атаки компанія CloudFlare розподілила трафік між своїми дата-центрами, після чого Cyberbunker зрозуміла, що не зможе «покласти» CloudFlare і почала нову хвилю атаки на її вищі бенкети. Деяка частина пакетів відфільтрувати на рівні Tier2, інший трафік потрапив на рівень Tier1, де потужність і досягла свого максимуму в 300 Гбіт / с. У цей момент мільйони користувачів мережі Інтернет відчули на собі всю міць цієї атаки, у них гальмували деякі сайти. В результаті провайдери витримали цю атаку, але в Європі було зареєстровано деяке збільшення пінгу при доступі до різних сайтів. Наприклад, в лондонському центрі обміну трафіку LINX 23 березня через атаки швидкість обміну даними впала більш ніж в два рази. Середня швидкість в 1.2 Тбіт / с впала до 0.40 Тбит / с.

2.1.7 Захист від DDoS-атак

Повністю захиститися від DDoS-атак на сьогоднішній день неможливо, так як абсолютно надійних систем не існує. Тут також велику роль відіграє людський фактор, тому що будь-яка помилка системного адміністратора, неправильно налаштовані маршрутизатор, може привести до дуже плачевних наслідків. Однак, незважаючи на все це, на даний момент існує маса як апаратно-

програмних засобів захисту, так і організаційних методів протистояння. Заходи протидії DDoS-атакам можна розділити на пасивні і активні, а також на превентивні і реакційні. Нижче наведено короткий перелік основних методів.

– Запобігання. Профілактика причин, що спонукають тих чи інших осіб організовувати і зробити DDoS-атаки. (Дуже часто кібератаки взагалі є наслідками особистих образ, політичних, релігійних та інших розбіжностей, що провокує поведінки жертви і т. П.). Потрібно вчасно усунути причини DDoS-атак, після цього зробити висновки, щоб уникнути таких атак в майбутньому.

– Відповідні заходи. Застосовуючи технічні та правові заходи, потрібно якомога активніше впливати на джерела і організатора DDoS-атаки. В даний час навіть існують спеціальні фірми, які допомагають знайти не тільки людини, який провів атаку, але навіть і самого організатора.

– Програмне забезпечення. На ринку сучасного програмного і апаратного забезпечення існує і таке, яке здатне захистити малий і середній бізнес від слабких DDoS-атак. Ці кошти зазвичай являють собою невеликий сервер.

– Фільтрація і блекхолінг. Блокування трафіку, що виходить від атакуючих машин. Ефективність цих методів знижується в міру наближення до об'єкта атаки і підвищується в міру наближення до атакуючої машині. В цьому випадку фільтрація може бути двох видів: використання міжмережевих екранів і списків ACL. Використання міжмережевих екранів блокує конкретний потік трафіку, але не дозволяє відокремити «хороший» трафік від «поганого». ACL списки фільтрують другорядні протоколи і не зачіпають протоколи TCP. Це не уповільнює швидкість роботи сервера, але марно в тому випадку, якщо зловмисник використовує першорядні запити.

– Зворотний DDOS - перенаправлення трафіку, використовуваного для атаки, на атакуючого. При достатній потужності атакується сервера дозволяє не тільки успішно відбити атаку, але і вивести з ладу сервер атакуючого.

– Усунення вразливостей. Чи не працює проти флуд-атак, для яких «вразливістю» є кінцівку тих чи інших системних ресурсів. Дана міра націлена на усунення помилок в системах і службах.

– Нарощування ресурсів. Абсолютного захисту, природно, не дає, але є хорошим фоном для застосування інших видів захисту від DDoS-атак.

– Розосередження. Побудова розподілених і дублювання систем, які не припинять обслуговувати користувачів, навіть якщо деякі їх елементи стануть недоступні через DoS-атаки.

– Ухилення. Відведення безпосередньої мети атаки (доменного імені або IP-адреси) подалі від інших ресурсів, які часто також піддаються впливу разом з безпосередньою метою атаки.

– Активні заходи у відповідь. Вплив на джерела, організатора або центр управління атакою, як техногенними, так і організаційно-правовими засобами.

– Використання обладнання для відображення DDoS-атак. Наприклад, DefensePro® (Radware), SecureSphere® (Imperva), Периметр (МФІ Софт), Arbor Peakflow®, Riorey, Impletec iCore і від інших виробників. Пристрої розгортаються перед серверами і маршрутизаторами, фільтруючи вхідний трафік.

– Придбання сервісу по захисту від DDoS-атак. Актуально в разі перевищення флудом пропускної спроможності мережевого каналу.

2.1.8 Статистика

Експерти «Лабораторії Касперського» провели дослідження і з'ясували, що в 2015 році DDoS-атаці піддалася кожна шоста російська компанія. За даними фахівців, протягом року було скоєно близько 120 тисяч атак, які були спрямовані на 68 тисяч ресурсів по всьому світу. У Росії кіберзлочинці найчастіше вибирали своєю мішенню великий бізнес - 20% випадків, середній і малий бізнес - 17%. DDoS-атаки були націлені на створення проблем в роботі головної сторінки сайту компаній (55% атак), виведення з ладу комунікаційних сервісів і пошти (34%), функції, що дозволяють користувачеві увійти в систему (23%). Також експерти з'ясували, що 18% DDoS-атак зафіксовано на файлові сервери і 12% -

на послуги по здійсненню фінансових операцій. Росія займає п'яте місце в світі за кількістю DDoS-атак на її сайти. Більша кількість кіберзлочинів відбувається в Китаї, США, Кореї та Канаді. Однак атаки найчастіше відбуваються китайськими і російськими хакерами.

2.2 Сучасні DDoS атаки

Сценарії сучасних мережевих атак часом нагадують детектив. Підозра спочатку падає на невинних, а лиходій успішно маскується до тих пір, поки за нього спільно не візьмуться професіонали. Експерти компанії Check Point опублікували звіт про розслідування інциденту з використанням нового методу атак на Linux-сервери. У ньому наводиться аналіз тактики зловмисників і використаних ними шкідливих програм, а також даються поради щодо захисту від них, пише Компьютерра.

У липні 2015 року з групою розслідування інцидентів Check Point зв'язався великий замовник, який виявив дивні дії в файлової системі на одному зі своїх серверів DNS BIND, які працювали під управлінням ОС Linux. Дивина полягала у великій кількості специфічних файлів, записаних в системних каталогах.

В результаті аналізу експерти встановили, що раніше в тому ж місяці сервер піддався Брутфорс облікових записів SSH. Його особливість полягала в тому, що атакуючих IP-адрес було дуже багато, і майже всі вони належали китайськими подсетям. Стандартні методи бана по IP виявилися неефективні. Кожен вузол встигав перебрати лише кілька паролів, але завдяки масованій атаці через кілька днів було отримано рутовий доступ.

Використовуючи рут, атакуючі впровадили на сервер троян XOR.DDoS і бекдор Groundhog. Вони «зомбують» заражені машини, роблячи їх частиною ботнету, який в подальшому використовується для проведення масштабних DDoS-атак і інших цілей.

Експерти відзначають майстерність авторів цих шкідливих програм і цілеспрямованість виконаної атаки. Більшість інших троянів і бекдор

поширюються хаотично, інфікуючи будь вразливі системи незалежно від їх ролі. Ці ж заражали лише сервери під управлінням Linux з потенційним доступом до швидкісних каналах. Висока пропускна здатність кожного з заражених серверів в ботнет дає можливість проводити DDoS-атаки небувалою інтенсивністю.

Цікаво, що на момент розслідування інциденту троян XOR.DDoS вже був відомий, а ось Groundhog став відкриттям. В результаті аналізу стало очевидно, що вони мають багато спільного на рівні конфігурації, методів захисту та способів комунікації. Глибоке вивчення їх коду дозволяє зробити висновок, що троян і бекдор мають спільне походження.

Згідно з попередніми розслідуванням, брутфорс SSH часто починався в підмережі, що належить китайській компанії HEE THAI LIMITED (AS63854). У квітневому звіті згадується про блокування її трафіку і позбавлення ботнету можливості настання. Проте останнє дослідження Check Point показало, що зловмисникам вдалося перевести свій ботнет-трафік в підмережа CHINANET, чиї сервери розміщені в провінції Цзянсу.

Подальший аналіз логів зараженого сервера і моніторинг його активності підтвердив, що зловмисники нещодавно змінили підмережі. Вони перестали використовувати ті ж IP-адреси, що і для початкового Брута SSH. Згідно з даними, зібраними в ході розслідування службою Check Point ThreatCloud, це був не єдиний випадок зараження, а керована розподілена кампанія, спрямована на сервери по всьому світу.

Процедура зараження серверів складалася з двох основних етапів: Брута SSH і інфікування набором з трояна і бекдора. Спочатку виконувалося впровадження XOR.DDoS. Цей троянець найчастіше використовується в сучасних DDoS-атаках, підтримуючи такі поширені методи, як SYN Flood, ACK Flood і DNS amplification. Цілі і параметри атак йому передає C & C-сервер, з яким XOR.DDoS підтримує розширене взаємодія: він може приймати і відправляти файли, виконувати скрипти і встановлювати інші шкідливі компоненти. Шифрування з'єднання з C & C зводиться до банальної процедури XOR, відображеної в назві трояна.

Однак для успішного наповнення ботнету мало заразити черговий сервер. Троян може бути виявлений, а пароль доступу змінений в будь-який момент, тому зловмисники також використовували функції бекдор Groundhog, щоб забезпечити собі постійний доступ. Його основне завдання полягає в віддаленому управлінні конфігурацією сервера, прийомі командних повідомлень і файлів, які він також може запускати на виконання. Для маскування зв'язок з C & C відбувається через різні порти TCP: 22, 80, 443 та інші. Groundhog використовує зумовлений домен GroUndHog.MapSnode.CoM (211.110.1.32), в честь якого він і отримав свою назву.

Опинившись на сервері, трояни здійснюють кілька дій, що забезпечують їх повторну активацію в разі перезавантаження. Скрипт автозавантаження створюється в папці /etc/init.d. Інший скрипт розміщується за адресою /etc/cron.hourly/gcc.sh і застосовується для щогодинної перевірки наявності троянів в системі. Ще один скрипт відповідає за примусове включення всіх мережевих інтерфейсів і застосовується для запуску раніше завантажених шкідливих файлів.

В сучасних атаках часто використовуються відразу декілька шкідливих програм. Кожна з них окремо виглядає черговим трояном, мережевим черв'яком або бекдор, що спеціалізуються на певному типі цілей - від смартфонів і домашніх ПК до маршрутизаторів і високопродуктивних серверів. Однак їх вміле поєднання відкриває для атакуючих зовсім інші можливості побудови ботнетів і виконання цілеспрямованих атак.

Розслідування останніх інцидентів показують, що ботнети стали найбільш досконалим засобом проведення DDoS-атак. Входять до їх складу вузли - лише інфіковані машини, чиї власники зазвичай не знають про несанкціоноване використання їх потужностей. Тому не слід сприймати їх як ініціаторів атаки. Щоб знайти її справжнє джерело, треба відновити весь ланцюжок подій. Складно виявити реальних ляльководів - тих, хто наповнював ботнет зараженими вузлами для подальшого продажу C & C або особистого використання.

Фахівці CheckPoint відзначають, що останнім часом змінився характер відомих кіберзагроз та виникло безліч нових. Великі організації все частіше стають жертвами цілеспрямованих атак, серед яких основну масу складають масштабні DDoS-атаки підвищеної складності. Через розподіленого характеру і застосування в них заражених серверів з високошвидкісними каналами, такі атаки важко блокувати класичними низькорівневими інструментами.

3 НАЛАШТУВАННЯ СЕРВЕРА ТА SSH З’ЄДНАННЯ

3.1 Основні відомості про ssh

SSH – Secure SHell[6]. Виходячи з назви, можна зрозуміти, що мова йде про певне безпечне середовище. Це мережевий протокол прикладного рівня. Характерною рисою даного протоколу є можливість шифрувати паролі і дані при їх передачі. Також дозволяє передавати будь-який інший протокол. Перша версія цього протоколу була розроблена ще в далекому 1995-му році, але так як в ньому було виявлено масу вразливосте, тому вже в 1996-му році була випущена друга версія з промовистою назвою SSH-2. Вона не сумісна з першою версією і тому, коли ми говорим про SSH то йдеться саме про SSH-2. З тих пір SSH не особливо змінила стандарти своєї роботи і широко використовується по цей час

Переваги SSH протоколу:

– дозволяє працювати віддалено на комп'ютері через командну оболонку.

– шифрування здійснюється за допомогою різноманітних алгоритмів.

– SSH дозволяє безпечно передавати практично будь-який мережевий протокол, це дає можливість передавати по зашифрованому каналу звукові та відео файли.

– стискає файли для їх подальшого шифрування і передачі.

– захищає передачу даних по каналу і практично запобігає будь-яку можливість включення в установлену сесію і перехопити дані.

Для роботи з SSH необхідний SSH-сервер і SSH-клієнт

SSH-сервер приймає з'єднання від клієнтських машин і проводить автентифікацію. Автентифікація на SSH проводиться трьома способами:

– За IP адресою, не самий безпечний спосіб, так як є можливість підміни IP адреси.

– За допомогою публічного ключа клієнта - принцип майже такий же, як при перевірці IP, тільки в даному випадку перевіряється ключ клієнта і ім'я користувача.

– Використовуючи пароль клієнта - основний метод перевірки. Пароль передається в зашифрованому вигляді.

3.2 Встановлення та налаштування OpenSSH на операційній системі Kali Linux

3.2.1 Встановлення сервісу OpenSSH

Перед налаштуванням та побудовою SSH з’єднання потрібно перевірити чи наявний цей сервіс на системі. Це робиться командою[2]:

service --status-all

Результат команди наведений на рисунку 3.1.

Рисунок 3.1. – Результат команди service --status all

Для встановлення потрібно ввести команду:

apt-get install -y openssh-server

Далі перевіряємо наявність ssh сервісу командою:

service --status all

Результат команди наведений на рисунку 3.2.

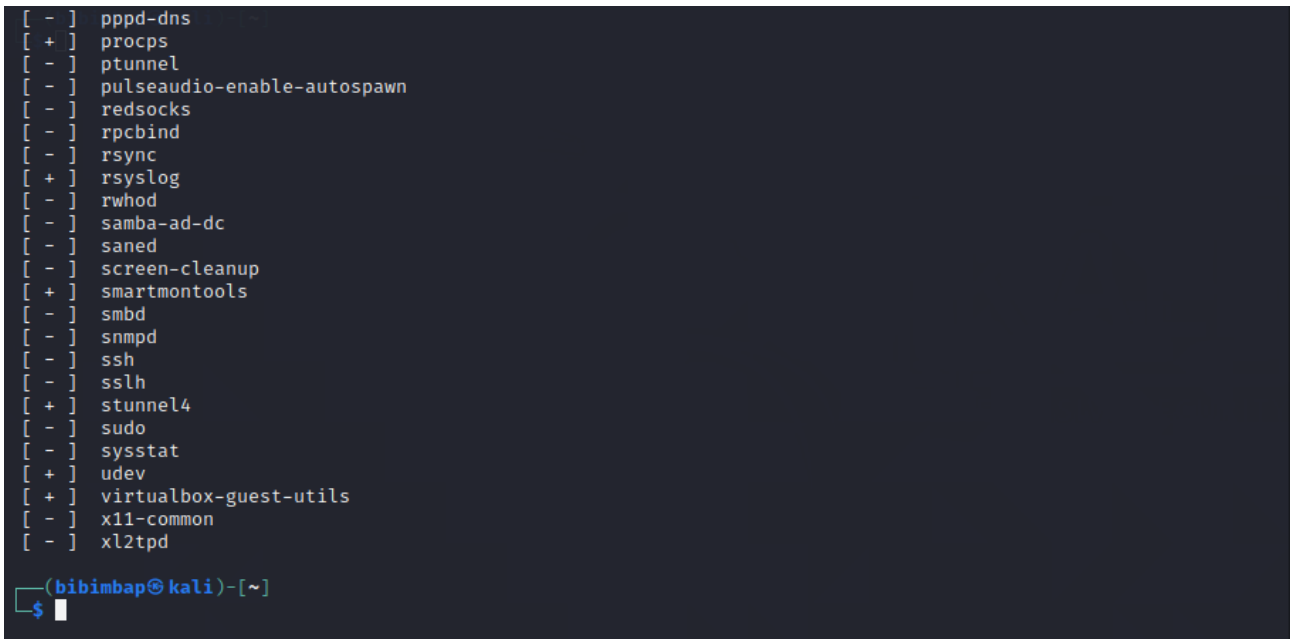

Рисунок 3.2 Результат команди service --status all після встановлення сервісу

Бачимо що сервіс наявний, але не включений. Для запуску сервісу необхідно ввести команду:

service ssh start

Далі перевіряємо статус сервісу командою:

service --status all

Результат команди наведений на рисунку 3.3.

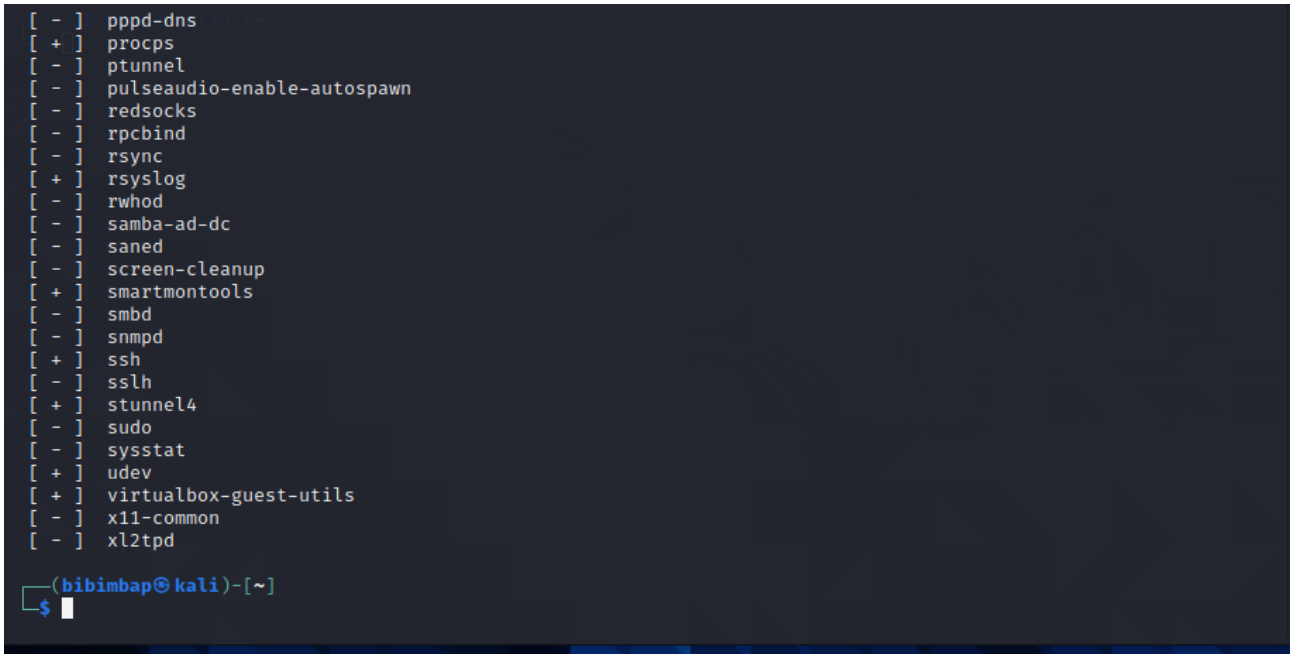

Рисунок 3.3 Статус сервісу ssh

Бачимо що ссервіс запущений. Тепер можна почати налаштування.

3.2.2 Налаштування сервісу OpenSSH

Для встановлення SSH з’єднання необхідно згенерувати пари ключів. Для генерування є можливість використати декілька алгоритмів[2].

Генерування пари ключів виконується за такою командою:

ssh-keygen -t rsa

Результат команди наведений на рисунку 3.4.

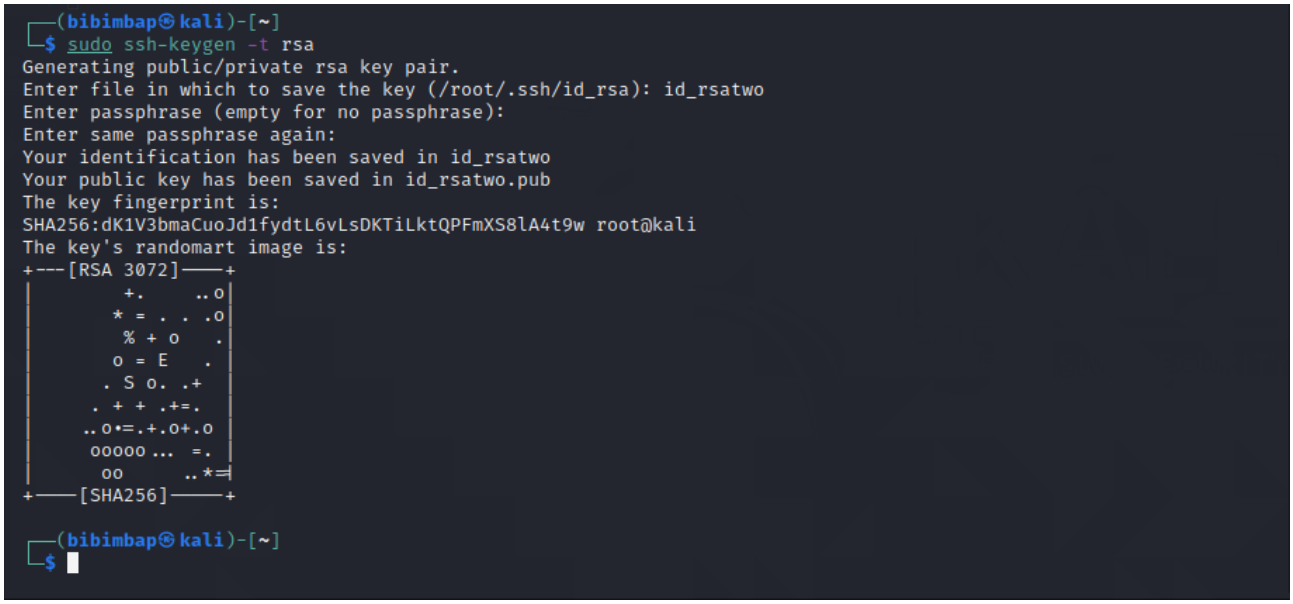

Рисунок 3.4 – Результат генерування пари ключів RSA

ssh-keygen -t dsa

Результат команди наведений на рисунку 3.5.

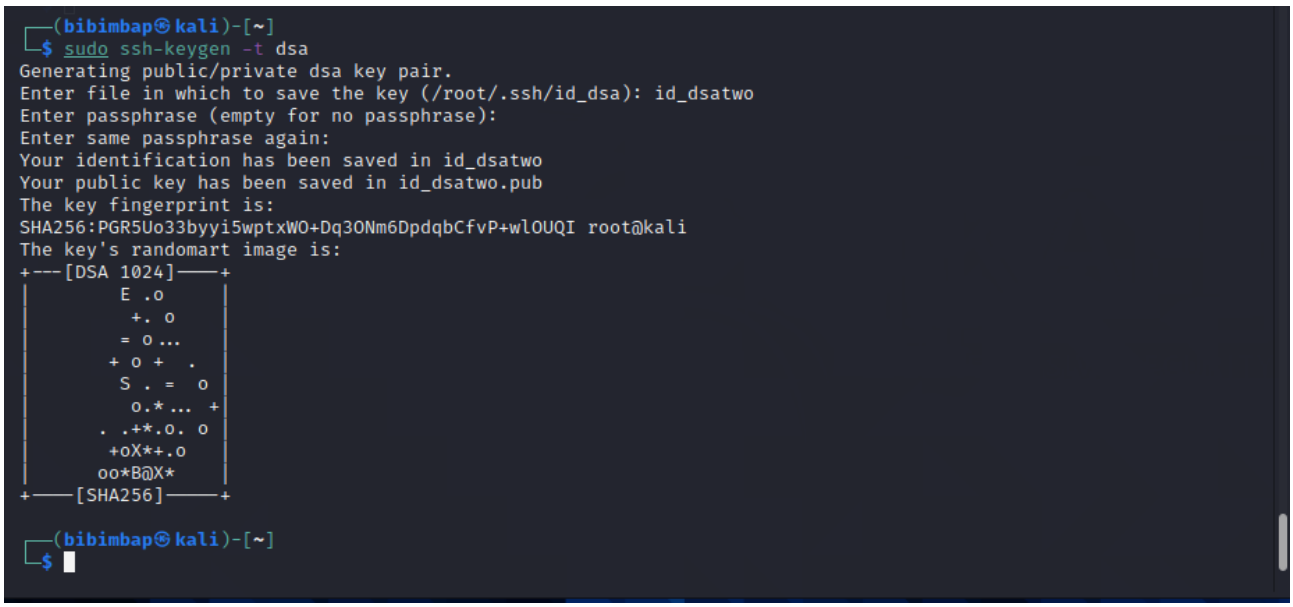

Рисунок 3.5. – Результат генерування пари ключів DSA

ssh-keygen -t ecdsa

Результат команди наведений на рисунку 3.6.

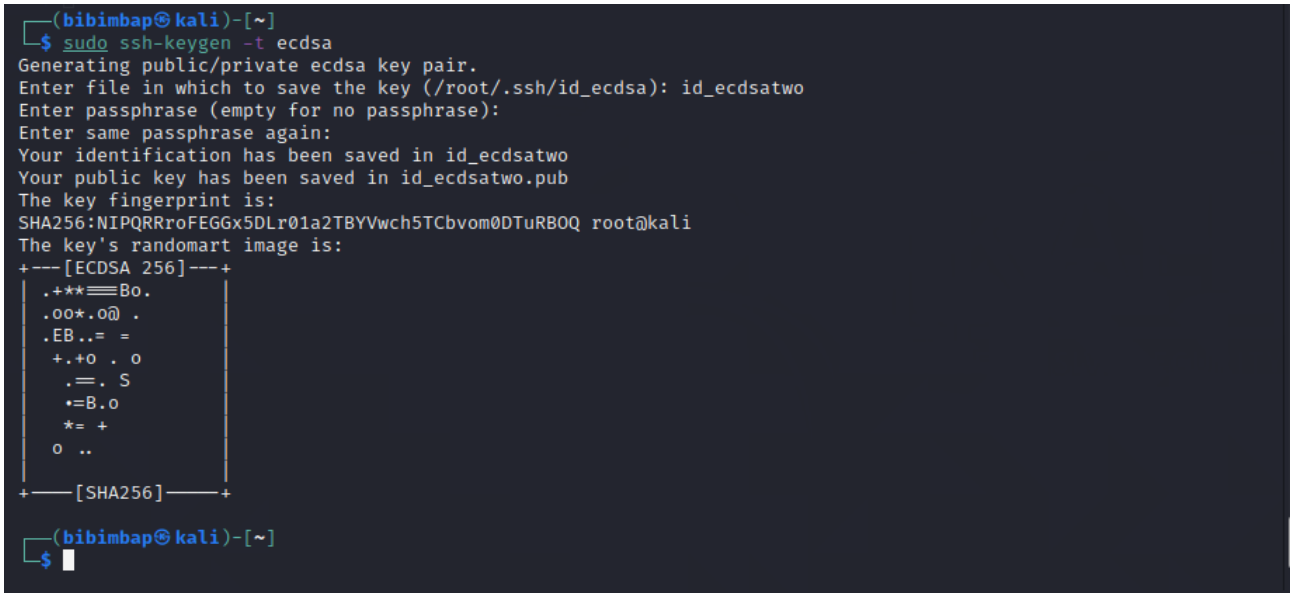

Рисунок 3.6 – Результат генерування пари ключів ECDSA

Після генерації пари ключів потрібно передати їх на інший вузол. Робиться це такою командою:

ssh-copy-id user@hostname

де. user – користувач під яким ми будемо працювати

hostname – ім’я узла на який будемо заходити

Параметри user та hostname редагуються на кожному вузлі у файлі hosts який знаходится за щляхом /etc/hosts:

Файл hosts має таку структуру:

1. Nodename username IP
2. Nodename username IP

……...

N. Nodename username IP

В якості параметра user виступає username, а в якості параметра hostname виступає параметр nodename або IP.

3.3 Налаштування SSH на системі CentOS 8.

3.3.1 Встановлення сервісу OpenSSH.

Для встановлення ввобимо команду[4]:

yum install –y openssh-service

Для підключення сервісу вводмо команду:

systemctl start sshd.service.

Для автоматичного запуска сервісу sshd потрібно написати таку команду:

systemctl enable sshd.service

3.3.2 Генерація та налаштування sshd

Генерація пари ключів здійснюється так як у пункті 3.2.2. Для передачі ключа на інший вузол необхідно написати команду[4]:

ssh-copy-id user@hostname

де. user – користувач під яким ми будемо працювати

hostname – ім’я вузла на який будемо заходити

3.4 Налаштування web-серверу apache

HTTP-сервер Apache - самий широко використовуваний веб-сервер в світі. Він має безліч потужних функцій, включаючи динамічно завантажувані модулі, надійну підтримку різних медіаформатів і інтеграцію з іншим популярним програмним забезпеченням.

3.4.1 Встановлення сервісу apache

Встановлення сервісу відбувається командою:

sudo dnf install httpd

Далі необхідно відкрити порти 80 иа 443. Для того щоб це зробити вводимо такі команди:

sudo firewall-cmd --permanent --add-service=https

sudo firewall-cmd --permanent --add-service=http

sudo firewall-cmd --reload

```
[root@localhost dahyun]# firewall-cmd --zone=public --permanent --add-service=ht
tp
success
[root@localhost dahyun]#
```

Рисунок 3.7 Відкриття порта 80.

3.4.2 Перевірка вед-сервера apache

Для запуска сервера необхідно ввести такі команди:

sudo systemctl start httpd

Та перевіряємо що відповідна служба працює:

sudo systemctl status httpd

```
[root@localhost dahyun]# systemctl status httpd
● httpd.service - The Apache HTTP Server
   Loaded: loaded (/usr/lib/systemd/system/httpd.service; disabled; vendor pres>
   Active: active (running) since Thu 2020-12-03 23:51:53 EET; 12min ago
     Docs: man:httpd.service(8)
 Main PID: 7069 (httpd)
   Status: "Total requests: 6; Idle/Busy workers 100/0;Requests/sec: 0.00833; B>
    Tasks: 214 (limit: 11324)
   Memory: 24.8M
   CGroup: /system.slice/httpd.service
           ├─7069 /usr/sbin/httpd -DFOREGROUND
           ├─7080 /usr/sbin/httpd -DFOREGROUND
           ├─7081 /usr/sbin/httpd -DFOREGROUND
           ├─7082 /usr/sbin/httpd -DFOREGROUND
           ├─7083 /usr/sbin/httpd -DFOREGROUND
           └─7084 /usr/sbin/httpd -DFOREGROUND

Dec 03 23:51:52 localhost.localdomain systemd[1]: Starting The Apache HTTP Serv>
Dec 03 23:51:53 localhost.localdomain httpd[7069]: AH00558: httpd: Could not re>
Dec 03 23:51:53 localhost.localdomain systemd[1]: Started The Apache HTTP Serve>
Dec 03 23:51:53 localhost.localdomain httpd[7069]: Server configured, listening>
lines 1-20/20 (END)
```

Рисунок 3.8 Перевірка працездатності відповідної служби

Далі за допомогою команди дізнаємося зовнішній та внутрішній ip:

Ifconfig

У пошуковому рядку вводимо http://server_ip

Якщо все зроблено правильно то на веб-сторінці побачимо рисунок 3.9

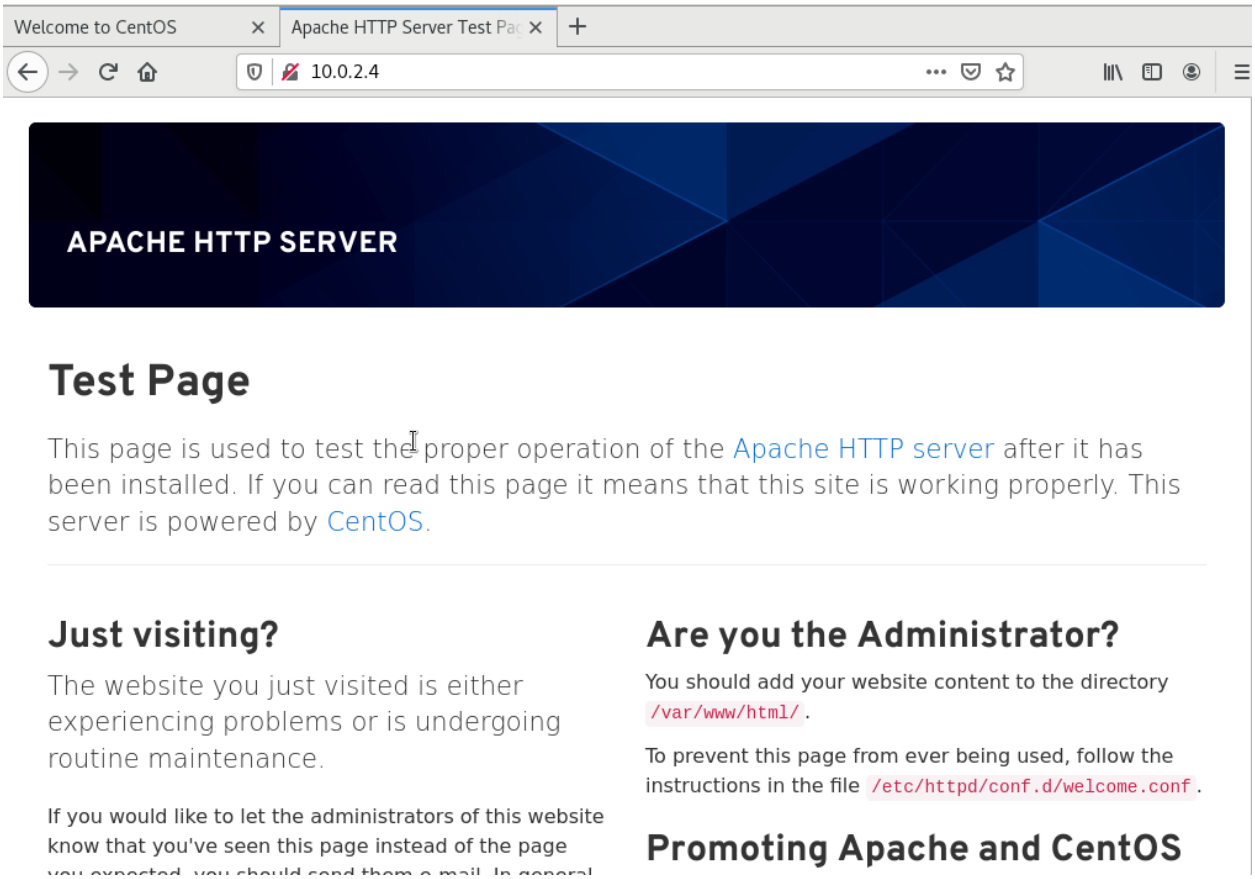

Рисунок 3.9 Тестова сторінка для перевірки роботи apache

Тепер необхідно налаштувати веб-сторінку. Зробити це нескладно. Необхідно за допомогою наступної команди, використовуючи будь-який текстовий редактор, створити файл index.html у каталозі /var/www/html та покласти в нього html код:

Sudo nano /var/www/html/index.html

Рисунок 3.10 Вміст файла index.html

Тоді на веб-сторінці побачимо рисунок 3.11

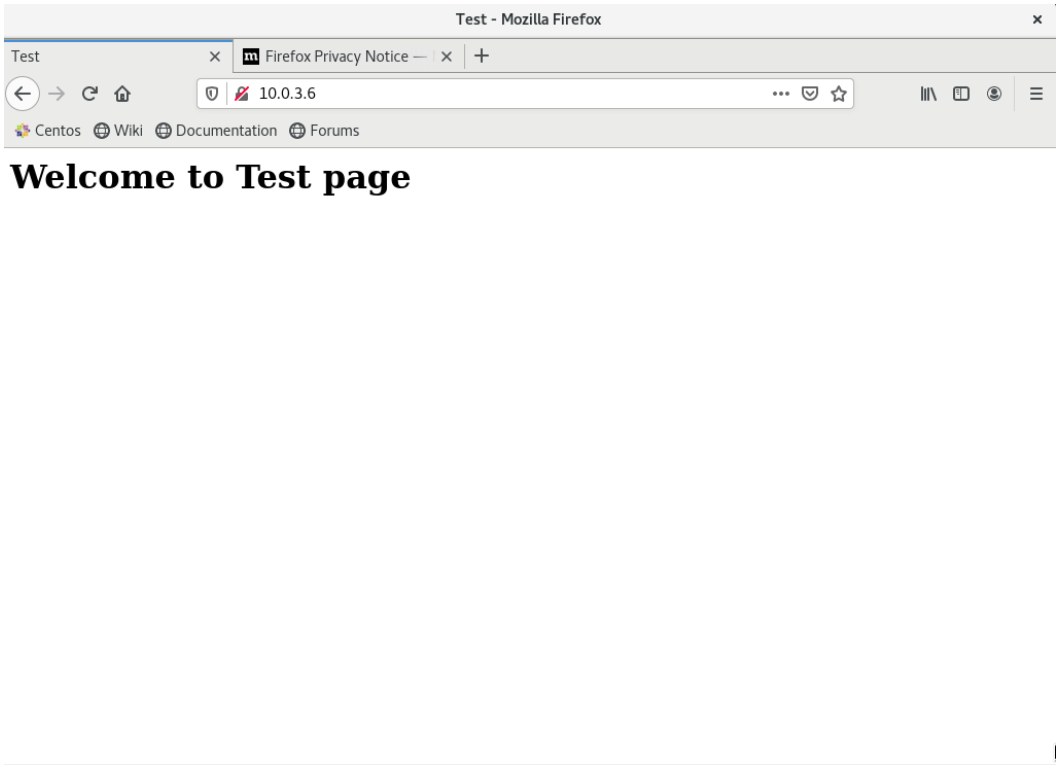

Рисунок 3.11 Вміст веб-сторінки index.html.

4 РЕАЛІЗАЦІЯ ТА МЕТОДИ ЗАХИСТУ ВІД BRUTE FORCE АТАК

Традиційні Unix системи зберігають дані про користувачів разом із зашифрованим паролем в текстовому файлі /etc/passwd. Оскільки цей файл використовується багатьма інструментальними засобами (типу ls) щоб відобразити власника файлу і інші подібні відомості, файл повинен бути відкритий на читання для всіх, що, звичайно, дає відмінний шанс зловмисникам[7].

Інший метод зберігання інформації – затінення паролів. Як і раніше, є файл /etc/passwd з даними про користувачів. Однак, замість паролів ставиться символ "x", а паролі зберігаються окремо в файлі /etc/shadow, в якому зберігаються зашифровані паролі і деяка додаткова інформація про паролі. Файл /etc/shadow доступний для читання лише root, що підвищує захист.

Файл /etc/passwd зберігає інформацію про користувачів в виде:

test:x:561:561:Anton:/home/smithj:/bin/bash

– ім’я користувача, до 8 символів. Регістр важливий, зазвичай пишуть в нижньому регістрі;
– символ "x" в поле пароля. Паролі зберігаються в файлі /etc/shadow
– числовий id користувача
– числовий id групи
– Повне ім'я користувача
– Домашній каталог користувача
– Призначена для користувача оболонка

Файл /etc/shadow зберігає дані про користувача в форматі:

test:Ep6mckrOLChF.:10063:0:99999:7:::

Як і в файлі passwd, кожне поле у файлі shadow відділяється двокрапкою:

– ім’я користувача, до 8 символів
– пароль, 13 символів (зашифрований). Порожня запис показує, що для входу пароль не потрібен

– кількість днів, коли пароль був змінений в останній раз.

– число днів до зміни пароля

– число днів, після яких пароль повинен бути змінений

– число днів, протягом яких користувач отримує попередження про необхідність пароль змінити

– число днів після закінчення дії пароля, коли ще можна працювати.

– число днів, після яких пароль буде заблокований.

– зарезервовано для можливого майбутнього використання.

4.1 Організація атаки за допомогою John The Riper

Як було описано вище дані про користувачів і паролі знаходяться у файлах password та shadow. Для отримання паролю з файла shadow по-перше потрібно використати команду unshadow[9]:

Результат команди наведений на рисунку 4.1.

Рисунок 4.1 – Використання команди unshadow

Тепер потрібен список паролів який знаходиться /usr/share/john/password.lst Kali Linux. Також можно використовувати список rockyou.txt або інші.

Далі вводимо комаду jhon –wordlist=/usr/share/john/password.lst /filename

Для виведення списку паролів у термінал потрібно ввести наступну команду:

John –show ~/filename

4.2 Мережевий підбір паролю по ssh

4.2.1 Підбір пароля за допомогою Hydra

Для цього необхідно знати IP адресу “жертви” та список паролів.

Вводимо до терміналу команду:

hydra -V -f -t 4 -l test -P /root/wordlist ssh://10.0.2.3

де: -V – показувати пару логін + пароль під час перебору

-f – зупинка як тільки буде знайдений пароль для зазначеного логіна

-P –шлях до словника з паролями

Ssh – вказівка сервіса і IP-адреса жертви

Результат команди наведений на рисунку 3.2.

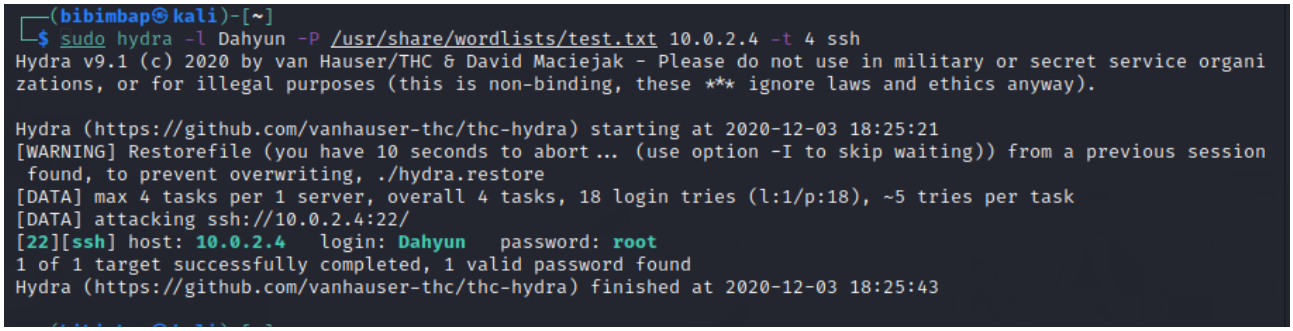

Рисунок 4.2 – Результат підбору програми Hydra

4.3 Організація DoS атаки за допомогою GoldenEye

4.3.1 Встановлення програмного забезпечення

Для встановлення утиліти необхідно створити директорію:

mkdir goldeneye

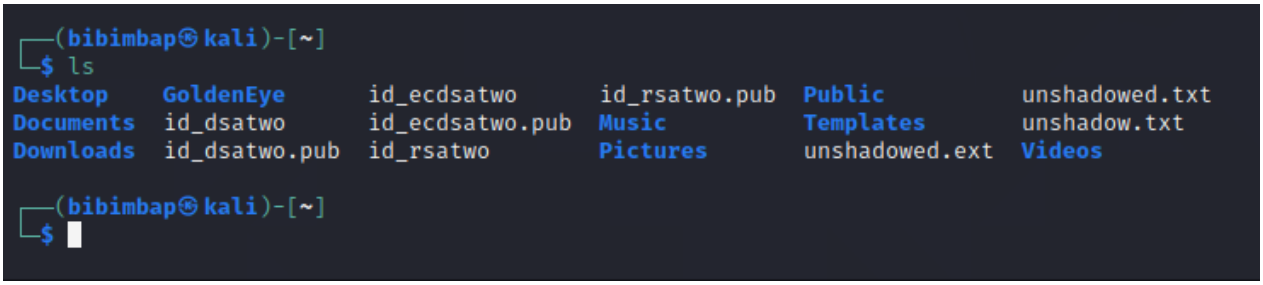

Рисунок 4.3 Результат створення директорії GoldenEye

Тепер переходимо в нього та качаємо архів:

cd GoldenEye

wget hyyps://github.com/jseidl/GoldenEye/archive/master.zip

Далі розпаковуємо архів:

unzip master.zip

Програма готова для використання. Запуск програми:

./goldeneye

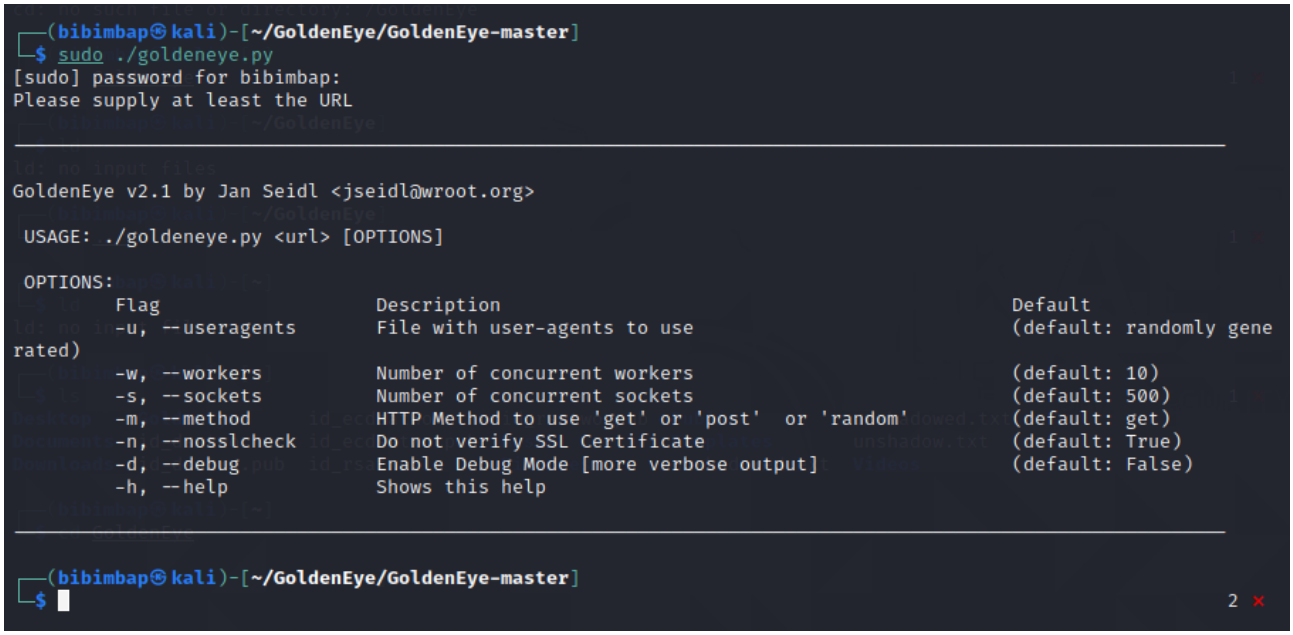

Рисунок 4.4 Результат запуска програми.

4.3.2 Проведення DoS атаки

./goldeneye.py http://ip-adress

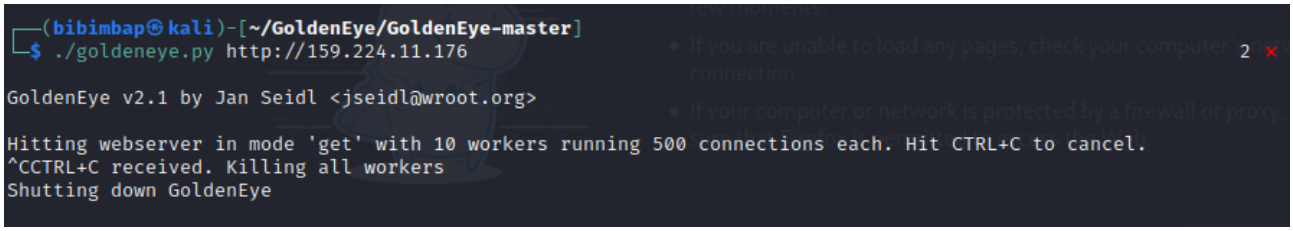

Рисунок 4.5 Виконання DDoS атаки

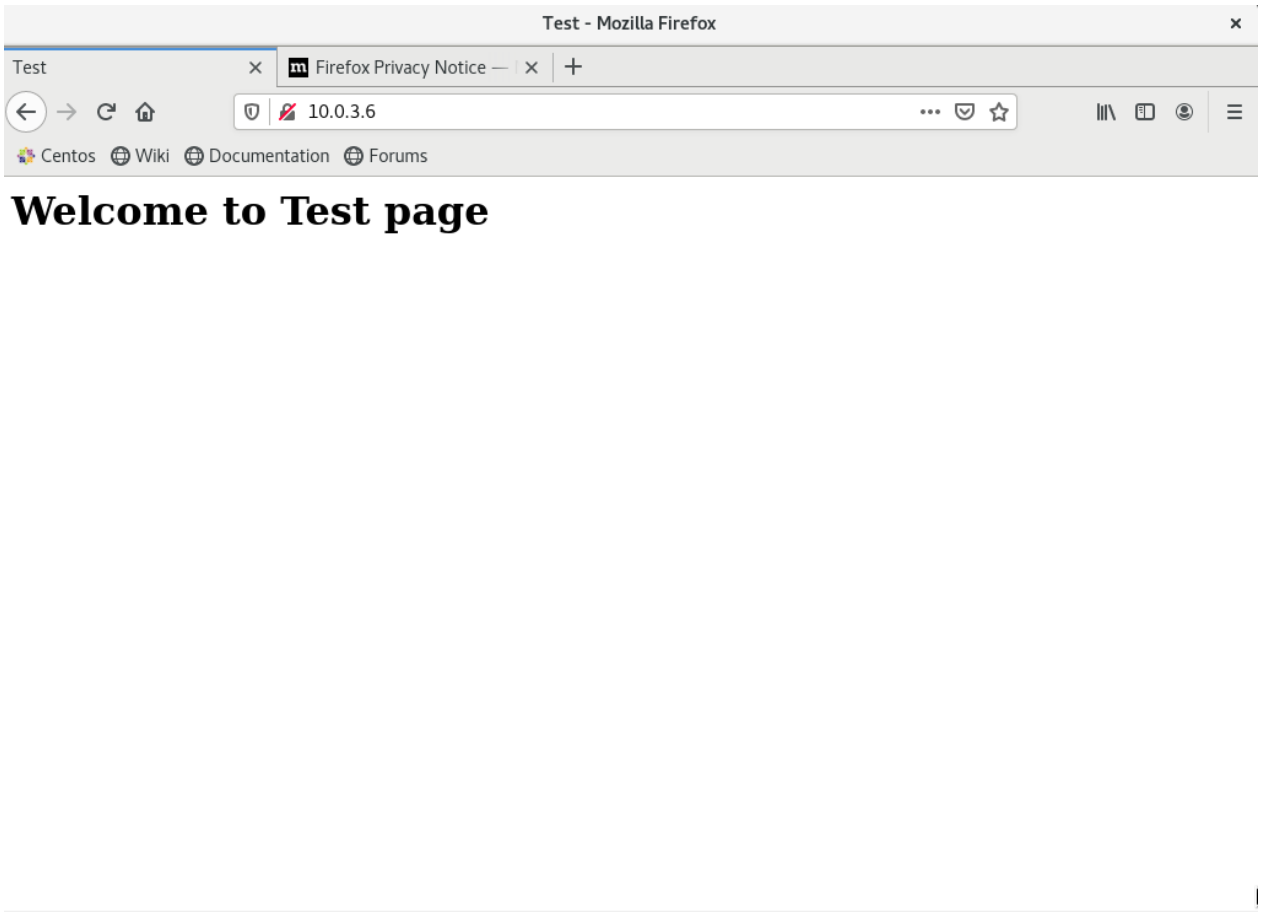

Рисунок 4.6 Стан серверу до атаки

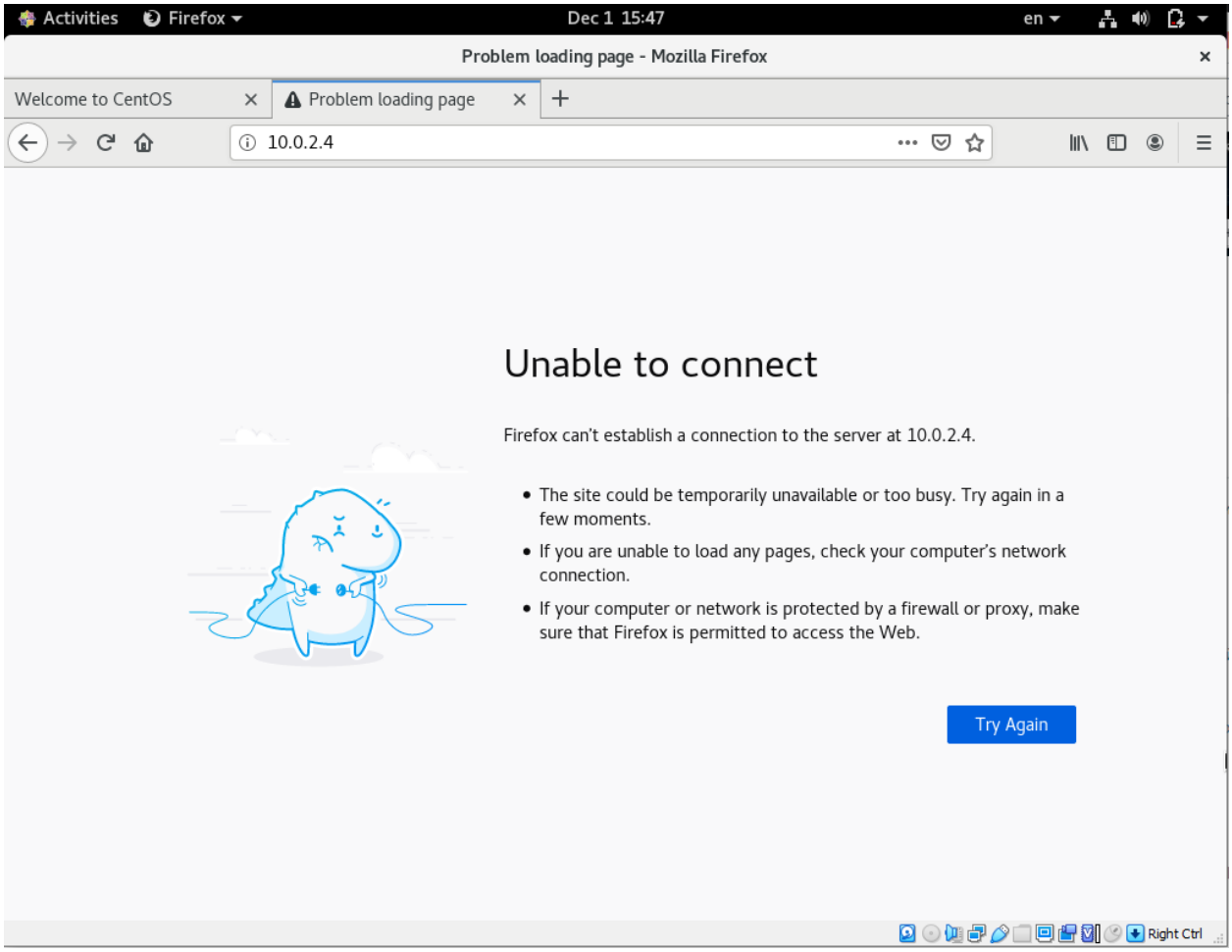

Рисунок 4.7 Стан серверу після атаки.

4.4 Методи захисту від bruteforce та DDoS атак

4.4.1 Локальний захист від bruteforce атаки

Для локального захисту файлу паролів passwd необхідно перевести його у формат shadow необхідно як суперкористувач ввести[7]:

/usr/sbin/pwconv

Після цього в структурі файла passwd хеш пароля змінится на X, а дані користувачів остануться незмінними. Хеш пароля буде перенесений до файла shadow, до якого мас доступ лише суперкористувач.

Внаслідок того що файл являється недоступним для звичайних користувачів, навіть якщо зловмисник буде знаходитися в систему доступу до суперкористувача він не отримає.

Brutforce атаки не будуть мати сенсу тому що до файлу shadow доступу не має, а в файлі passwd немає ніякої інформації про паролі.

4.4.2 Мережевий захист

Для мережевого захисту, а зокрема від вторгнення із мережі на сервер або на вузол має сенс використовувати утиліти fail2ban[3].

Fail2ban у реальному часі сканує лог файли системи та на усі запити з'єднання по протоколам ssh, telnet або інших, з невірним паролям видає тимчасовий бан після вичерпання кількості спроб. Та повідомляє адміністратора про підозрілу активність у мережі. Якщо спроби з'єднання продовжуються то IP адреса з якої приходять запроси, заноситься в чорний список.

Для установлення fail2ban необхідно встановити необхідний додатковий пакет EPEL. Для цього потрібно написати команду

sudo yum install -y epel-release

Після можна встановити fail2ban:

sudo yum install -y fail2ban

Далі необхідно підключити цю службу.

sudo systemctl enable fail2ban

Тепер можна налаштувати роботу служби fail2ban. Для цього використовуються такі файли:

/etc/fail2ban/jail.conf

/etc/fail2ban/jail.d/*.conf,

/etc/fail2ban/jail.local

/etc/fail2ban/jail.d/*.local.

Файл jail.conf не редагуэтся, тому що цей файл зберігає стандартні настройки оновлюються при оновлені утиліти. Замість нього необхідно створити файли jail.local який буде перевизначать jail.conf.

Для переналаштування файлу jail.conf треба змінити файл jail.local. В файл необхідно додати такі строки:

[DEFAULT]

#Кількість секунд на які буде забанен хост

bantime =

Override /etc/fail2ban/jail.d/00-firewalld.conf:banaction = iptables-multiport

#Максимальна кількість спроб з’єднання

maxretry =

#Включення sshd

[sshd]

enabled = true

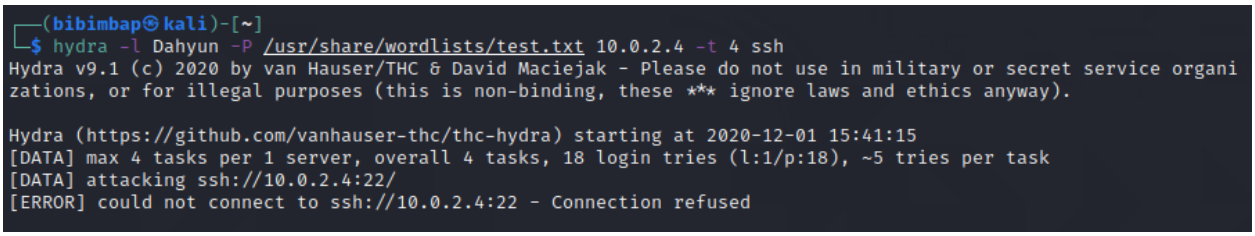

Рисунок 4.8 Результат атаки при включеному fail2ban.

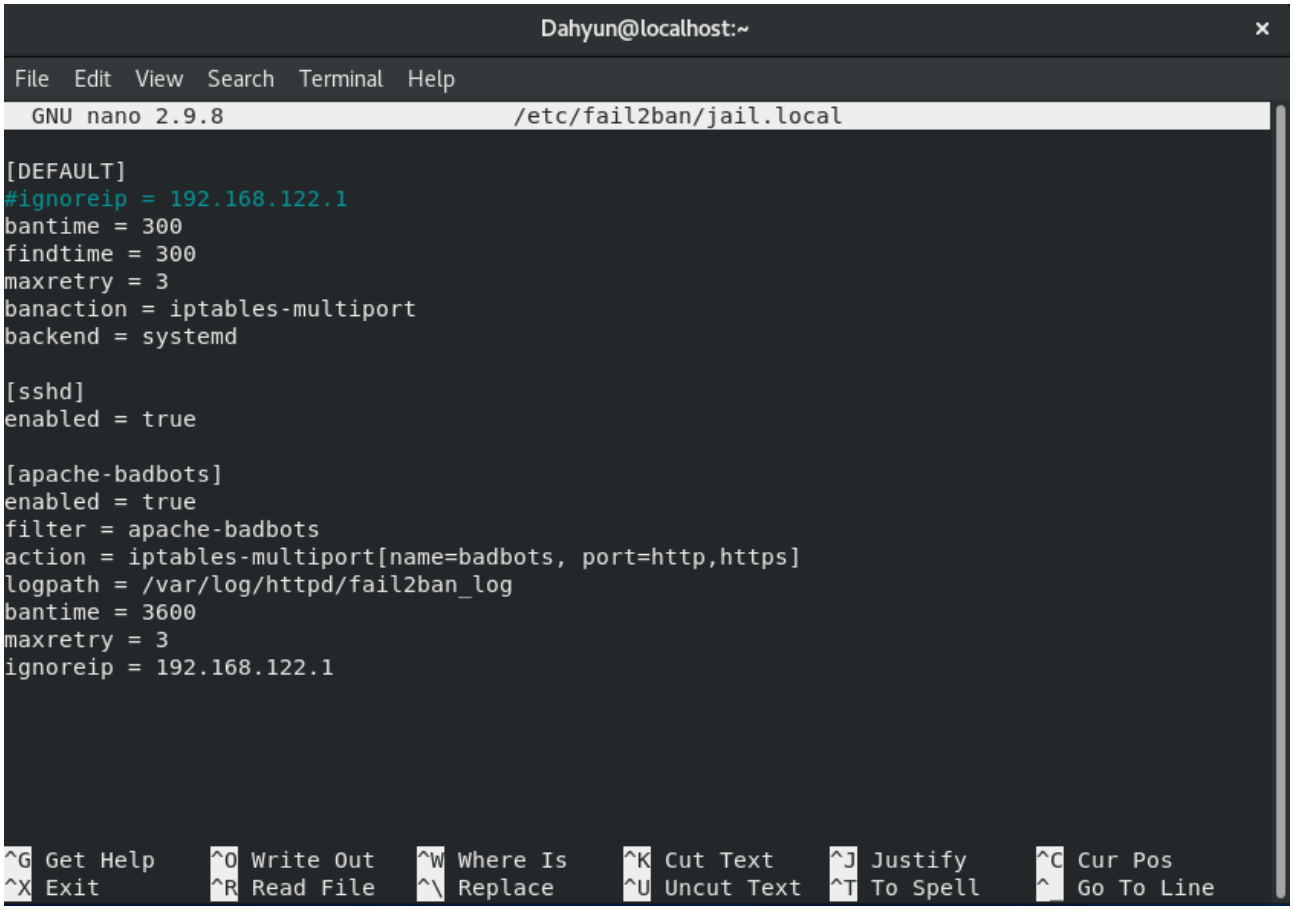

Рисунок 4.9 Конфігурація jail.conf

4.5 Статистика

Характеристика системи на якої проводилися тестування:

– Intel(R) Core(TM) i5-3317U CPU @ 1.70 GHz

– ОЗУ 8 Гб

– Жорсткий диск 250 Гб

Емуляція проводилася на віртуальній системі за допомогою програми Oracle VirtualBox.

Таблиця 4.1 Статистика brute force атак.

	Час	Кі-ть спроб	Кі-ть вдалих спроб	Процент
Brute с захистом	-	100	0	0%
Brute без захисту	30~хв	100	76	76%

Таблиця 4.2 Статистика DDoS атак.

	Час	Кі-ть спроб	Кі-ть вдалих спроб	Процент
DDoS с захистом	-	100	0	0%
DDoS без захисту	5~хв	100	11	11%

ВИСНОВКИ

В магістерській роботі був встановлений веб-сервер apache на Unix ОС CentOS 8. Налаштований згідно інструкції написаній в роботі. Виконані мінімальні налаштовування безпеки та протестовані на за допомогою утиліт системи Kali linux таких як hping3 та goldeneye.

Під час виконання роботи сервер вийшов з ладу лише в 11% випадків. Це сталося через недостатність ресурсів робочої станції. Але після встановлення необхідного програмного забезпечення випадків коли сервер вийшов з ладу було 0. Для захисту від DDoS атак я використовував спеціальну утиліту fail2ban. Ця утиліта дозволяє встановити обмеження для відповідних сервісів.

На практиці має сенс налаштовувати fail2ban на 3 спроби входу в коротких проміжок часу, блокувати IP на 48 годин. Також є гарна утиліта яка відправляє повідомлення на електронну пошту в разі розпізнавання підозрілої діяльності.

Були розглянуті методи протидії bruteforce атакам по ssh з’єднанню. Розроблений алгоритм захисту від brutforce атак, та видвинуто рекомендації для захист.

Також в роботі тестувалися методи захисту від bruteforce атак. Brute force використовував оригінальних словник, створений на базі словник rockyou, який зберігає найбільш популярніші паролі в світі. За основу був взят саме цей словник бо на сьогодні більшість людей не змінюють паролі на роутері не кажучи про IoT речі або електронну пошту.

Підбор паролів без захисту вдавався в 76% випадків. Але після налаштування fail2ban жодна з спроб не була успішною. Fail2ban на сервіс ssh налаштований на такі параметри: кількість спроб – 3, бан ip – 5 хв.

Також є один важливий момент в налаштуванні ssh з’єднання. В файлі sshd_config, який знаходиться в каталозі /etc/ssh/ є налаштування: #PermitRootLogin yes. В первісному налаштуванні ssh необхідно поставити її на “no”. Якщо цього не зробити, то без необхідних заходів захисту хто завгодно може отримати root доступ до сервера.

Fail2ban – є гарною утилітою для забезпечення безпеки з’єднання по ssh, та протидії DDoS атакам. Рекомендовані налаштування: 3-5 спроб входу, від 5 хв. бану з подальшим збільшенням часу обмеження входу для ssh з’єднання, та від 24 год бану для DDoS атак.

Рекомендовано використовувати формат shadow для зберігання паролів, через підвищену безпеку, обмеження доступу до файлу, та змоги змінити локацію файлу.

Рекомендації до паролів такі як в міжнародному стандарті:

– Кількість символів в паролі повинна бути від 8 до 15.

– В паролі повинні використовуватися символи верхнього регістру.

– Необхідно змінювати свій пароль з тривалістю 1-2 місяці.

– Непоганим може бути перевірка свого пароля зі словником, наприклад, rockyou, але це ресурсозатратна дія.

ПЕРЕЛІК ПОСИЛАНЬ

1. В.А. Шеховцов Операційні системи [Текст] / В.А. Шевцов – НБУВ, 2005 126 с.
2. Налаштування SSH-сервера на Kali Linux або BackTrack [Електронний ресурс] / cryptoparty – Режим доступа: www/ URL: https://itsecforu.ru/2018/02/08/настройка-ssh-сервера-на-kali-linux-или-backtrack/ - 08.02.2018 р. – Електрон дані та загл с екрана.
3. Налаштування fail2ban [Електронний ресурс] / Режим доступу www/ URL: https://vps.ua/wiki/install-linux-vps/security/configuring-fail2ban/#a-4-1 – 18.03.2017 р. - Електрон дані та загл с екрана.
4. Налаштування SSH [Елктронний ресурс] / Режим доступу www/ URL: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/system_administrators_guide/s1-ssh-configuration/ - 05.05.2019 р. – Електронні дані та загл с екрана.
5. Official Kali Linux Documentation [Електронний ресурс] / Режим доступу www/ URL: https://www.kali.org/kali-linux-documentation/ - 07.06.2019 р. – Електронні дані.
6. Родерик В. Смит Сетевые средства Linux [Текст] / Родерик В. Смит – Видання “Вильямс”2003 672 с.
7. Праолі в Linux та формат файла shaow [Електронний ресурс] / Макси Чирков – Режим доступу www/ URL: https://www.opennet.ru/docs/RUS/lame/x822.html - 23.02.2019 р. - Електронні дані.
8. Уязвимости операционных систем [Електронний ресурс] / Дмитро Кікот – Режи доступу www/ URL: https://habr.com/ru/company/ua-hosting/blog/407979/ - 09.10.2017 р. – Електронні дані.
9. Інструкція використання John The Riper [Електронний ресурс] / Режим доступу www/ URL: https://hackware.ru/?p=411 – 20.12.2015 р. – Елекуронні дані.

10. Інструменти Kali Linux Hydra [Електронний ресурс] / Режим доступу www/ URL: https://kali.tools/?p=1847 – 10.06.2019 р. – Електронні дані.
11. Як атакують Linux-сервери [Електронний ресурс] / Режим доступу www/ URL: https://dev.by/news/kak-hakery-atakuyut-linux-servery-i-zametayut-sledy - Електронні дані
12. The DDoS that almost Broke the Internet [Електронний ресурс] / Режим доступу www/ URL: https://cloudflare.com/the-ddos-that-almost-broke-the-internet/ - Електронні дані
13. Deep Inside a DNS Amplification DDoS Attack [Електронний ресурс] / Режим доступу www/ URL: https://cloudflare.com/deep-inside-a-dns-amplification-ddos-attack/ - Електронні дані
14. DDoS через DNS-резольвери [Електронний ресурс] / Режим доступу www/ https://xakep.ru/2012/10/31/59564/ - Електронний ресурс
15. Denial of Service Attacks [Електронний ресурс] / Режим доступу www/ URL: https://s2.ist.psu.edu/paper/DDoS-Chap-Gu-June-07.pdf - Електронні дані
16. Apache HTTP server project [Електронний ресурс] / Режим доступу https://httpd.apache.org/ - Електронний ресурс