МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Київський національний університет будівництва та архітектури

ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Методичні вказівки
до виконання лабораторних робіт
для студентів спеціальностей 123 «Комп'ютерна інженерія»
та 125 «Кібербезпека»

Київ 2023

УДК 004.56.5 (043.2)

Укладачі: С.В. Кондакова, канд. фіз-мат наук, доцент;
А.М. Кондакова, аспірант

Рецензент: Є.Є. Шабала, канд. техн. наук, доцент

Відповідальний за випуск Ю.І. Хлапонін, д-р. техн. наук, професор

Затверджено на засіданні кафедри кібербезпеки та комп'ютерної інженерії протокол №6 від 31 січня 2023р.

В авторській редакції.

Технології створення та застосування систем захисту інформації : методичні вказівки / уклад.: С.В. Кондакова, А.М. Кондакова – Київ: КНУБА, 2023. – 32 с.

Містять зміст, порядок оформлення і вказівки до виконання лабораторних робіт.

Призначено для студентів спеціальностей 123 «Комп'ютерна інженерія» та 125 «Кібербезпека» галузі знань 12 «Інформаційні технології»

ЗМІСТ

ВСТУП

Працюючи на посадах, пов’язаних з системною безпекою необхідно знати, розуміти та розробляти принципи кібергігієни в організації. Для цього потрібно розуміти базові принципи, якими користуються хакери-зловмисники. Зрозуміло що завжди зловмисники йдуть на крок попереду та неможливо запобігти атакам нульового дня, але завдання системних адміністраторів та посад близьких за значенням, є зменшення можливостей успішного проведення даних атак.

Уявімо що ми «білі хакери». Завдання лабораторних робіт пояснити принцип роботи зловмисників та зрозуміти варіанти захисту від них. Адже набагато легше захищати мережу, коли відомі варіанти її злому.

Працюючи над завданнями лабораторних робіт звертаю увагу на дотримання Законодавства України у сфері кібербезпеки.

- Попереджую про проведення робіт виключно для навчання та виключно зі згоди іншої особи.
- Нагадую про Законодавство України у сфері кіберзахисту та кібербезпеки, Кримінальний кодекс України (статті 361, 362, 363, 190)

ОСНОВНІ ВИЗНАЧЕННЯ ТА ТЕРМІНИ:

Основні терміни та визначення, що будуть вживатись в процесі навання наведено згідно Закону України "Про захист інформації в інформаційно-комунікаційних системах".

блокування інформації в системі - дії, внаслідок яких унеможливлюється доступ до інформації в системі;

витік інформації - результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї;

власник інформації - фізична або юридична особа, якій належать права на інформацію;

власник системи - фізична або юридична особа, якій належить право власності на систему;

доступ до інформації в системі - отримання користувачем можливості обробляти інформацію в системі;

захист інформації в системі - діяльність, спрямована на запобігання несанкціонованим діям щодо інформації в системі;

знищення інформації в системі - дії, внаслідок яких інформація в системі зникає;

інформаційна (автоматизована) система - організаційно-технічна система, в якій реалізується технологія обробки інформації з використанням технічних і програмних засобів;

інформаційно-комунікаційна система - сукупність інформаційних та електронних комунікаційних систем, які у процесі обробки інформації діють як єдине ціле;

комплексна система захисту інформації - взаємопов'язана сукупність організаційних та інженерно-технічних заходів, засобів і методів захисту інформації;

користувач інформації в системі (далі - користувач) - фізична або юридична особа, яка в установленому законодавством порядку отримала право доступу до інформації в системі;

криптографічний захист інформації - вид захисту інформації, що реалізується шляхом перетворення інформації з використанням спеціальних (ключових) даних з метою приховування/відновлення змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

несанкціоновані дії щодо інформації в системі - дії, що провадяться з порушенням порядку доступу до цієї інформації, установленого відповідно до законодавства;

обробка інформації в системі - виконання однієї або кількох операцій, зокрема: збирання, введення, записування, перетворення, зчитування, зберігання, знищення, реєстрації, приймання, отримання, передавання, які здійснюються в системі за допомогою технічних і програмних засобів;

порушення цілісності інформації в системі - несанкціоновані дії щодо інформації в системі, внаслідок яких змінюється її вміст;

порядок доступу до інформації в системі - умови отримання користувачем можливості обробляти інформацію в системі та правила обробки цієї інформації;

електронна комунікаційна система - сукупність технічних і програмних засобів, призначених для обміну інформацією шляхом передавання, випромінювання та/або приймання її у вигляді сигналів, знаків, звуків, рухомих або нерухомих зображень чи в інший спосіб;

технічний захист інформації - вид захисту інформації, спрямований на забезпечення за допомогою інженерно-технічних заходів та/або програмних і технічних засобів унеможливлення витоку, знищення та блокування інформації, порушення цілісності та режиму доступу до інформації.

Терміни, що вживаються у Стратегії інформаційної безпеки, мають таке значення:

інформаційна безпека України - складова частина національної безпеки України, стан захищеності державного суверенітету, територіальної цілісності, демократичного конституційного ладу, інших життєво важливих інтересів людини, суспільства і держави, за якого належним чином забезпечуються конституційні права і свободи людини на збирання, зберігання, використання та поширення інформації, доступ до достовірної та об'єктивної інформації, існує ефективна система захисту і протидії нанесенню шкоди через поширення негативних інформаційних впливів, у тому числі скоординоване поширення недостовірної інформації, деструктивної пропаганди, інших інформаційних операцій, несанкціоноване розповсюдження, використання й порушення цілісності інформації з обмеженим доступом;

інформаційна загроза - потенційно або реально негативні явища, тенденції і чинники інформаційного впливу на людину, суспільство і державу, що застосовуються в інформаційній сфері з метою унеможливлення чи ускладнення реалізації національних інтересів та збереження національних цінностей України

і можуть прямо чи опосередковано завдати шкоди інтересам держави, її національній безпеці та обороні;

інформаційні заходи оборони держави - сукупність скоординованих дій, які готуються та здійснюються суб'єктами забезпечення національної безпеки і оборони України в мирний час, в особливий період, в умовах воєнного або надзвичайного стану щодо прогнозування та виявлення інформаційних загроз у воєнній сфері, запобігання, стримування та відсічі збройній агресії проти України, протидії інформаційним загрозам з боку держави-агресора, а також здійснення інших необхідних дій в інформаційному протиборстві;

антикризові комунікації - комплекс інформаційних заходів, що реалізуються державними органами України з метою запобігання виникненню кризової ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються загрози виникнення кризової ситуації і протидії їй;

кризові комунікації - комплекс заходів, що реалізуються державними органами України у кризовій ситуації і передбачають їх діалог із цільовою аудиторією з питань, що стосуються кризової ситуації і протидії їй;

стратегічні комунікації - скоординоване і належне використання комунікативних можливостей держави - публічної дипломатії, зв'язків із громадськістю, військових зв'язків, інформаційних та психологічних операцій, заходів, спрямованих на просування цілей держави;

стратегічний наратив - спеціально підготовлений текст, призначений для вербального викладення у процесі стратегічних комунікацій з метою інформаційного впливу на цільову аудиторію;

урядові комунікації - комплекс заходів, що передбачають діалог уповноважених представників Кабінету Міністрів України з цільовою аудиторією з метою роз'яснення урядової позиції та/або політики з певних проблемних питань.

Терміни, що вживаються Положенні "Про технічний захист інформації в Україні":

конфіденційність - властивість інформації бути захищеною від несанкціонованого ознайомлення;

цілісність - властивість інформації бути захищеною від несанкціонованого спотворення, руйнування або знищення;

доступність - властивість інформації бути захищеною від несанкціонованого блокування;

технічний захист інформації (ТЗІ) - діяльність, спрямована на забезпечення інженерно-технічними заходами конфіденційності, цілісності та доступності інформації;

інформаційна система - автоматизована система, комп'ютерна мережа або система зв'язку;

дозвіл - документ, що надає право на виконання робіт з технічного захисту інформації для власних потреб;

комплекс технічного захисту інформації - сукупність заходів та засобів, призначених для реалізації технічного захисту інформації в інформаційній системі або на об'єкті.

Терміни, що вживаються в Законі Про Державну таємницю:

державна таємниця (далі також - секретна інформація) - вид таємної інформації, що охоплює відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому цим Законом, державною таємницею і підлягають охороні державою;

віднесення інформації до державної таємниці - процедура прийняття (державним експертом з питань таємниць) рішення про віднесення категорії відомостей або окремих відомостей до державної таємниці з установленням ступеня їх секретності шляхом обгрунтування та визначення можливої шкоди національній безпеці України у разі розголошення цих відомостей;

гриф секретності - реквізит матеріального носія секретної інформації, що засвідчує ступінь секретності даної інформації;

допуск до державної таємниці - оформлення права громадянина на доступ до секретної інформації;

доступ до державної таємниці - надання повноважною посадовою особою дозволу громадянину на ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, або ознайомлення з конкретною секретною інформацією та провадження діяльності, пов'язаної з державною таємницею, цією посадовою особою відповідно до її службових повноважень;

засекречування матеріальних носіїв інформації - введення у встановленому законодавством порядку обмежень на поширення та доступ до конкретної секретної інформації шляхом надання відповідного грифу секретності документам, виробам або іншим матеріальним носіям цієї інформації;

категорія режиму секретності - категорія, яка характеризує важливість та обсяги відомостей, що становлять державну таємницю, які зосереджені в державних органах, органах місцевого самоврядування, на підприємствах, в установах і організаціях;

криптографічний захист секретної інформації - вид захисту, що реалізується шляхом перетворення інформації з використанням спеціальних даних (ключових даних) з метою приховування (або відновлення) змісту інформації, підтвердження її справжності, цілісності, авторства тощо;

матеріальні носії секретної інформації - матеріальні об'єкти, в тому числі фізичні поля, в яких відомості, що становлять державну таємницю, відображені у вигляді текстів, знаків, символів, образів, сигналів, технічних рішень, процесів тощо;

охорона державної таємниці - комплекс організаційно-правових, інженерно-технічних, криптографічних та оперативно-розшукових заходів, спрямованих на запобігання розголошенню секретної інформації та втратам її матеріальних носіїв;

ступінь секретності ("особливої важливості", "цілком таємно", "таємно") - категорія, яка характеризує важливість секретної інформації, ступінь обмеження доступу до неї та рівень її охорони державою;

технічний захист секретної інформації - вид захисту, спрямований на забезпечення інженерно-технічними заходами конфіденційності, цілісності та унеможливлення блокування інформації.

ЛАБОРАТОРНІ ЗАВДАННЯ

Лабораторна робота №1 Методи виявлення вразливостей систем та мереж

Проблематика, завдання та цілі виконання лабораторної роботи

Першим базовим кроком при підготовці кібератак є проведення соціальної інженерії. Не рідко траплялися випадки, коли система була досить захищеною, мала мінімум вразливостей, але атаку на неї вдалось виконати успішно завдяки, наприклад, фотографії співробітника організації, опублікованій на його сторінці в соціальній мережі, де на задньому фоні лежав листок, з записаним паролем чи введення в якості пароля входу в систему імені домашнього улюбленця, перед тим успішно опублікованого для всіх зацікавлених. Тож шляхом використання фішингу, вдається зібрати велику кількість інформації про особу.

Практичні рекомендації для виконання

Фішинг: Один з основних методів соціальної інженерії — фішинг — полягає у створенні масової інтернет-розсилки нібито від імені відомої організації. У класичній схемі фішингу користувач отримує email з «обґрунтованою» вимогою пройти за посиланням на підставний сайт з метою авторизації. У листі може бути прохання змінити пароль або повідомити дані банківської картки. Жертва шахрайства не розуміє, що потрапляє на фішинговий ресурс, і надає запитувану інформацію.

Троян: Ця техніка полягає у проникненні шкідливої програми в комп'ютер жертви. Суть полягає в наступному: на пошту надходить лист із пропозицією отримати додатковий дохід, виграш, компромат на колегу, оновлення антивірусу або іншу «приманку». Завантажуючи програму, користувач заражає свій пристрій вірусом, здатним збирати або змінювати наявну інформацію. Файл ретельно маскується, тому розпізнати підробку вдається не кожному: саме тому «троянського коня» вважають одним з методів соціальної інженерії.

Кві про кво: Свою назву цей метод отримав від латинського словосполучення «quid pro quo», що в перекладі означає «послуга за послугу». Алгоритм дій злочинця наступний: він дзвонить користувачеві, представляється співробітником технічної підтримки та повідомляє про збої в роботі програмного забезпечення. Звісно, ніяких неполадок немає, але довірлива людина намагається допомогти та виконує вказівки зловмисника, тим самим надаючи доступ до важливої інформації.

Претекстинг: Ще один метод соціальної інженерії. Претекстинг — це дія, відпрацьована за заздалегідь складеним алгоритмом. Щоб отримати потрібні дані, соціальний хакер видає себе за особу, відому потенційній жертві.

Зловмисники дзвонять громадянам і представляються співробітниками кредитно-фінансових організацій, кол-центрів або технічної підтримки. Щоб викликати довіру, шахраї повідомляють співрозмовнику інформацію про нього (наприклад, прізвище, посаду, дату народження) або про проєкти, з якими він працює. Іноді хакер представляється знайомим або членом сім'ї та просить швидко переказати кошти на вказаний рахунок.

Зворотна соціальна інженерія: Цей вид атаки спрямований на створення ситуації, коли жертва самостійно звертається до шахрая. Зазвичай злочинці досягають своєї мети двома шляхами: рекламуючи власні «послуги» або встановлюючи шкідливе ПЗ.

Впровадження особливого ПЗ: Схема кіберзлочинців спрямована на те, щоб користувач звернувся для розв'язання проблеми саме до них. Спочатку встановлена програма працює «як годинник», але з часом виникають неполадки. Виконуючи вказані шахраями дії, людина надає доступ до своїх даних. А коли виявляється факт витоку інформації, злочинець залишається поза підозрою, оскільки, на думку жертви, він просто надавав допомогу та виконував свою роботу.

Ще один приклад застосування методів соціальної інженерії — на пристрої можуть з'явитися діалогові вікна з повідомленням про збої або необхідність оновлення. Не підозрюючи про обман, користувач проходить за посиланням у діалоговому вікні або завантажує «нову версію» програми, тим самим встановлюючи шкідливий файл на свій комп'ютер.

Реклама: Найчастіше під час пошуків майстра ми покладаємось на власну інтуїцію та не завжди можемо об'єктивно оцінити роботу технічного спеціаліста. Цим користуються злочинці: рекламуючи послуги, вони створюють ситуацію, коли потенційна жертва змушена сама звернутися до них. Під виглядом ремонту або відновлення Windows шахрай може встановити вірусний файл або отримати доступ до конфіденційної інформації. Якщо хакер має задатки психолога, він може легко вивідати необхідні дані в процесі комунікації.

Завдання до лабораторної роботи

Завданням є з’ясувати можливість отримання критичної інформації про особу шляхом застосування різноманітних методів соціальної інженерії. Критичною є будь яка інформація, що може зацікавити вибрану особу, бути корисною для отримання інформації про паролі, систему, проблеми з її безпекою, тощо. Тобто про будь що, що може призвести до успішної атаки на систему, інтернет-ресурс тощо.

Попереджую про проведення робіт виключно для навчання та виключно зі згоди іншої особи. Нагадую про Законодавство України у сфері кіберзахисту та кібербезпеки, Кримінальний кодекс України (статті 361, 362, 363, 190)

Висновки та результати роботи

У висновках необхідно надати будь-яку критичну інформацію про особу чи організацію, що могла б допомогти при майбутніх атаках на мережу компанії.

Також необхідно описати механізми за якими була отримана така інформація. Це може бути ознайомлення з соціальними мережами працівників, проглядування фотографій на сайті компанії, надсилання фішингових листів.

В методиках проведення лабораторної роботи ви не обмежені. ПІСЛЯ ПОПЕРЕДНЬОГО УЗГОДЖЕННЯ З ЖЕРТВОЮ, ДЛЯ ДІЙ В МЕЖАХ ЗАКОНОДАВСТВА УКРАЇНИ.

Також як висновок необхідно подати варіанти використання отриманої інформації для проведення хакерських атак.

Відповідь має бути максимально наближеним результатом до справжнього першого етапу проведення хакерської атаки оформленим як звіт «білого хакера» керівнику піддослідної компанії.

Лабораторна робота №2 «Сканування мережі за допомогою Advanced IP Scanner»

Проблематика, завдання та цілі виконання лабораторної роботи

Сканування мережі відноситься до набору процедур для ідентифікації хостів, портів і служб, що працюють в мережі.

Сканування вразливостей визначає можливість атак мережевої безпеки. Оцінює мережі на наявність вразливостей, непотрібні послуги, слабку аутентифікацію і слабке шифрування. Сканування вразливостей є одним з найважливіших компонентів будь-якого завдання тестів на проникнення. Вам необхідно провести тестування на проникнення і надати список загроз та вразливостей, знайдені в мережі організації, виконати сканування портів, мережеве сканування і сканування вразливостей щоб визначити IP / ім'я хоста та його вразливості.

Мета цієї лабораторії полягає в вивченні проведення мережевого сканування, аналізу уразливості і підтримки безпеки мережі.

Грунтуючись на тому, що ми дізналися від збору нашої інформації і моделювання загроз, ми можемо почати активно аналізувати наші жертви на наявність вразливостей. Ми значно звузили нашу область атаки, так як ми вперше почали тестування на проникнення з усім потенціалом.

Зверніть увагу, що не всі уразливості приведуть до компрометації системи. При пошуку відомих вразливостей ви знайдете більше проблем які розкривають конфіденційну інформацію або можуть призвести до відмови в обслуговуванні, ніж уразливості, які призводять до віддаленого виконання коду. Насправді, навіть, здавалося б, нешкідлива конфігурація може бути поворотним моментом у випробуванні на проникнення, який надасть вам доступ.

Наприклад, розглянемо FTP анонімний доступ для читання. Це досить звичайна установка. Хоча FTP є небезпечним протоколом, і ми повинні в цілому направити наших клієнтів до використання більш безпечних варіантів, як SFTP, використовуючи FTP з анонімним читання саме по собі не призводить до компрометації. Якщо ви зіткнулися з сервером FTP, який дозволяє анонімний доступ для читання, але доступ для читання обмежується каталогом FTP, який не містить будь-яких файлів, які були б цікаві зловмисником, то ризик, пов'язаний з анонімним варіантом читання мінімальний. З іншого боку, якщо ви в змозі прочитати всю файлову систему за допомогою анонімного FTP клієнта, або, можливо, навіть гірше, хтось помилково залишив комерційну таємницю клієнта в каталозі FTP, який читається для анонімного користувача.

Сканери вразливостей широко використовуються в випробуванні на проникнення. Як ми побачимо в цій роботі, сканера вразливостей можуть допомогти в швидкому отриманні потенційно цікавої інформації.

У цій лабораторній роботі ми розглянемо кілька форм оцінки вразливостей. Дослідимо деякі часто використовувані інструменти сканування.

Практичні рекомендації для виконання

Виберіть організацію, яка на вашу думку, заслуговує уваги. Це може бути навчальний заклад, комерційна компанія, або, можливо, некомерційна благодійна організація (пам’ятаємо про Законодавство України).

Advanced IP Scanner - безкоштовна утиліта для управління корпоративними і домашніми мережами, що дозволяє за лічені секунди збирати інформацію про комп'ютери в мережі і знаходити їх різні ресурси, такі як загальні папки, HTTP, HTTPS і FTP. Завдяки інтеграції з програмою Radmin Advanced IP Scanner можна знаходити всі машини і підключитися до них в один клік.

Advanced IP Scanner це надійний та безкоштовний мережевий сканер для аналізу локальних мереж. Програма сканує всі пристрої в мережі, надає доступ до спільних папок та FTP-серверів, дає можливість віддалено управляти комп'ютерами (через RDP та Radmin), і навіть може віддалено вимикати їх. Advanced IP Scanner не потребує встановлення та має простий доброзичливий інтерфейс. Ця програма має бути присутня в арсеналі кожного системного адміністратора.

В наші дні, де зловмисники чекають шансу щоб атакувати організацію, щоб відключити її, стає дуже важливим сканування вразливостей, щоб знайти недоліки і уразливості в мережі і закрити їх, перш ніж зловмисник вторгнеться в мережу. Мета запуску сканера вразливостей полягає у визначенні пристроїв в мережі, які відкриті для відомих вразливостей.

Мета цієї лабораторії, допомогти студентам виконати локальне сканування мережі та виявити всі ресурси в мережі.

Вам потрібно:

- Сканер мережі
- Облікові записи користувачів
- Виконання віддаленого проникнення
- Збір інформації про комп'ютери в мережі

В лабораторній, вам необхідно:

Завантажити останню версію Advanced IP Scanner по посиланню http://www.advanced-ip-scanner.com чи схожу за методиками роботи програму.

Мережеве сканування виконується з метою збору інформації про систему, відкриті порти і мережеві вразливості. Зібрана інформація може допомогти у визначенні загроз і вразливостей в мережі і дізнатися, чи є яка-небудь підозрілі або несанкціоновані підключення, які можуть призвести до крадіжки даних і привести до пошкодження ресурсів.

Завдання:

1. Advanced IP Scanner сканує всі IP-адреса в межах і відображає результати сканування після завершення.
2. Ви можете бачити на малюнку, що Scanner Advanced IP детектує IP-адреса і відображає статус як живий.
3. Клацніть правою кнопкою миші будь-який з виявлених IP-адрес. Це буде список Wake-On-LAN, Shut down, та Abort Shut dow.
4. Ви можете примусово вимикати, перезавантажити і відмінити вимкнення машини / IP адреса.
5. Тепер у вас є IP-адреса, назва та інші деталі зараженого комп'ютера.

Висновки та результати роботи

Задокументуйте всі IP-адреси, відкриті порти і запущені програми і протоколи, виявлені в ході лабораторної роботи.

Інформація сканування:

- IP-адреса
- Системні імена
- MAC-адресу
- Виробник
- Стан системи

Лабораторна робота №3 «Ідентифікація виробника, моделі і версії сервера за допомогою ID Server»

Ідентифікація виробника, моделі і версії сервера за допомогою ID Server.

Цей інструмент також може бути використаний зловмисником для виявлення вразливостей, таких як переповнення буфера, ін'єкції SQL, і веб-додатків в мережі. Якщо ці уразливості не фіксуються, зловмисники можуть легко використовувати їх.

Використовуючи цей метод можна також знайти проблеми в захисту серверів або визначити ролі серверів в мережі. В цій лабораторній, ви навчитеся сканувати машину, щоб визначити віддалену цільову систему за допомогою ID Server.

Проблематика, завдання та цілі виконання лабораторної роботи

Метою лабораторної є допомога студентам навчити студентів ідентифіковувати виробника, модель і версію серверів:

В лабораторній ви вивчите:

- Визначення матриці домену IP-адреса.
- Визначення матриці інформації про домен.

Середовище

- Ви можете завантажити останню версію ID Server.
- Двічі клацніть idserve для запуску ID Server
- Ввімкніть адміністративні привілеї для запуску ID Server
- Запустіть цей інструмент на Windows Server 2012

Огляд ID Server

ID Server може підключитися до будь-якого порту сервера на будь-якому домені або IP-адресі, часто ідентифікує виробника, модель і версію сервера, будь то для FTP, SMTP, POP або будь-що інше.

Практичні рекомендації для виконання

1. В головному вікні ID Server виберіть вкладку Запит сервера.
2. Введіть IP-адресу або URL-адресу в поле Введіть або скопіюйте / вставте URL внутрішнього сервера або IP-адреса тут.
3. Натисніть Запит на сервер; він показує запит сервера обробленої інформації

Документуйте всі IP-адреси, їх запущені додатки, а також протоколи, виявлені в ході лабораторної роботи.

Висновки та результати роботи

У звіті надайте розгорнутий опис серверу на предмет виробника, версії і моделі серверу. Надати рекомендації щодо усунення або зменшення імовірності ознайомлення з критичною інформацією щодо серверу.

Лабораторна робота №4 «Моніторинг підключень TCP / IP за допомогою інструменту CurrPorts Tool»

CurrPorts це програма мережевого моніторингу, яка відображає список всіх відкритих TCP / IP і UDP портів на локальному комп'ютері

Проблематика, завдання та цілі виконання лабораторної роботи

У попередній лабораторії ви дізналися про етичного хакера, і ви повинні бути в змозі блокувати такі атаки з використанням відповідних брандмауерів або відключити непотрібні служби, запущені на комп'ютері.

Ви вже знаєте, що Інтернет використовує протокол програмного забезпечення під назвою TCP / IP для форматування і передачі даних. Зловмисник може контролювати поточні з'єднання TCP і може мати всю інформацію в заголовках IP і TCP і в мережах пакетної передачі корисних даних, з якими він або вона може захопити з'єднання. У міру того як зловмисник збирає інформацію про мережі, то він або вона може створити помилкові пакети в з'єднанні TCP.

Як адміністратора мережі, вашим щоденним завданням є перевірка TCP / IP з'єднання кожного сервера управління. Ви повинні контролювати всі TCP і UDP порти і список всіх встановлених IP-адреси сервера за допомогою інструменту CurrPorts.

Мета цієї лабораторії, допомогти студентам визначити і перерахувати всі TCP / IP і UDP портів на локальному комп'ютері.

Практичні рекомендації для виконання

В лабораторній роботі необхідно виконати:

- Сканування системи відкритого в даний момент TCP / IP і UDP портів
- Збір інформації про порти і процеси, які відкриті
- Список всіх IP-адрес, які встановлені з'єднання.
- Закрити небажані TCP з'єднання і вбити процес, який відкрив порти

Для виконання лабораторної роботи вам необхідно:

- Ви можете завантажити останню версію CurrPorts за посиланням HTTP: / / www.nirsoft.net/utils/cports.html
- Комп'ютер під керуванням Windows Server 2012
- Двічі клацніть cports.exe, щоб запустити цей інструмент
- Привілеї адміністратора для запуску програми CurrPorts

Огляд TCP/IP моніторингу за допомогою утиліти CurrPorts

Моніторинг TCP / IP портів перевіряє, чи існує кілька з'єднань IP встановлених портів TCP / IP сканування отримує інформацію про всіх відкриті TCP і UDP порти, а також відображає всі встановлені IP-адреси на сервері.

Утиліта CurrPorts є автономним виконуваний файл і не вимагає установки або додаткових бібліотек DLL (Dynamic Link Library). Встановіть CurrPorts в потрібне місце і двічі клацніть cports.exe для запуску.

1. Запуск CurrPorts. Він автоматично відображає ім'я процесу, порти, IP і віддалені адреси, і їх стан
2. CurrPorts перераховані всі процеси і їх ідентифікатори, використовувані протоколи, локальний і віддалений IP-адреси, локальні і видалені порти, а також вилучені імена хостів.
3. Для того, щоб переглянути всі звіти в вигляді HTML-сторінки, натисніть View -> HTML Reports – All items.
4. Для перегляду тільки обраного звіту у вигляді HTML-сторінки, виберіть звіти і натисніть , HTML Report – Selected items.
5. Для перегляду властивостей порту, виберіть порт і натисніть File -> Properties.
6. Натисніть кнопку OK, щоб закрити вікно Властивості
7. Щоб закрити з'єднання TCP які ви вважаєте підозрілим, виберіть процес і натисніть close Selected TCP Connections (Ctrl + T).
8. Для виходу з утиліти CurrPorts, натисніть Exit та вікно CurrPorts закриється.

Висновки та результати роботи

Документуйте всі IP-адреси, відкриті порти і їх запущені додатки та протоколи, виявлені в ході виконання лабораторної.

- Ім'я процесу
- ID процесу
- Протокол
- Локальний порт, локальна адреса
- Віддалений порт
- Віддалене ім’я порта
- Віддалена адреса
- Віддалене ім’я хоста

Проаналізуйте отриману інформацію та надайте рекомендації щодо підвищення захищеності мережі на основі проаналізованих даних.

Лабораторну роботу оформити як звіт керівнику організації про проведені дослідження разом з рекомендаціями.

Лабораторна робота №5 «Сканування мережі за допомогою Nmap, ZenNmap»

Вивчення і аудит мережі за допомогою **Nmap**.

Nmap (Zenmap є офіційним GUI Nmap) є вільним, відкритим вихідним кодом (ліцензія) утиліта для дослідження мережі та аудиту безпеки.

Огляд сканування мережі

Мережеві адреси перевіряються, щоб визначити:

- Які послуги (додатків імен та версія) ці хости пропонують
- Які операційні системи (ОС і версії) вони працюють
- Тип пакета фільтрів / брандмауерів, які використовуються і десятки інших характеристик

Проблематика, завдання та цілі виконання лабораторної роботи

В попередній лабораторії ви навчилися використовувати сканер мережі, щоб з'ясувати рівень вразливості, деталі для відкритих і закритих портів, уразливих комп'ютерів і т.д. адміністратора і зловмисник може використовувати ті ж інструменти, щоб виправити або експлуатувати систему. Якщо зловмисник дізнається всю інформацію про вразливих комп'ютерах, вони будуть діяти негайно, щоб поставити під загрозу ці системи з використанням методів розвідки.

Тому, як адміністратор, дуже важливо для вас, щоб виправити ці системи після того, як ви визначили всі вразливі місця в мережі.

Крім того, в якості етичного хакера і адміністратора мережі для вашої компанії, ваша робота полягає в тому, щоб виконувати щоденні завдання по забезпеченню безпеки, такі як інвентаризація мережі, розклад поновлення служби та моніторинг хоста або служби безвідмовної роботи. Таким чином, ви будете орієнтуватися в цій лабораторній, щоб використовувати Nmap для вивчення і аудиту мережі.

Мета цієї лабораторії, допомогти студентам вивчити і зрозуміти, як виконати мережеву інвентаризацію, управління послугами та поновлення, розклад мережевих завдання і моніторинг хоста або службу безвідмовної роботи і час простою.

Практичні рекомендації для виконання

В цій лабораторній, вам необхідно провести:

- Сканування TCP і UDP порти

- Аналіз деталей хостів і їх топологія
- Визначити типи фільтрів пакетів
- Записати і зберегти всі звіти сканування
- Порівняти збережені результати для підозрілих портів

Для виконання лабораторної роботи вам необхідно:

- Ви можете завантажити останню версію Nmap по посиланню http://nmap.org
- Комп'ютер під керуванням Windows Server 2012 в якості хост-машини
- Windows Server 2008 побудованого на віртуальній машині в якості гостя
- Веб-браузер з доступ до інтернету
- Адміністративні привілеї для запуску програми Nmap

Інсталювати мережевий сканер nmap

Установка утиліти виконується командою # apt-get install nmap

Сканування за допомогою програми Nmap дозволяє використовувати велику кількість функцій. Переглянути їх можна за допомогою команди nmap –h.

Провести скануваня мережі на визначення активних хостів

Для дослідів можна використати спеціальний хост, що створений безпосередньо розробниками nmap - scanme.nmap.org.

Ключі сканування задавати не обов’язково – в цьому випадку nmap перевірить хост на наявність відкритих портів та служб, які слухають ці порти.

Запустить можна командою: # nmap scanme.nmap.org

Через декілька секунд отримаємо результат:

Визначити операційну систему активного хосту

На активному хості провести сканування портів усіма методами

Nmap може сканувати різними методами – наприклад, UDP, TCP connect(), TCP SYN (напіввідкрите), FTP proxy (через ftp), Reverse-ident, ICMP (ping), FIN, ACK, SYN и NULL- сканування.

Вибір варіанта сканування залежить від вибраного ключа. Виклик nmap має наступний вигляд: nmap <ключі> ціль

-sS (TCP SYN сканування)

-sT (TCP сканування з використанням системного виклику connect)

-sU (різні типи UDP сканування)

-sN; -sF; -sX (TCP NULL, FIN и Xmas сканування)

- Null сканування (-sN)
- FIN сканування (-sF)
- Xmas сканування (-sX)

-sA (TCP ACK сканування)

-sW (TCP Window сканування)

-sM (TCP сканування (Maimon))
-sO (сканування IP протокола)

Графічним інтерфейсом програми Nmap, є програма **Zenmap.**

1. Введіть IP адресу віртуальної машини.
2. В профілі: текстове поле, виберіть зі списку тип профілю, який ви хочете переглянути, виберіть Intense Scan.
3. Натисніть кнопку Scan, щоб почати сканування віртуальної машини.
4. Zenmap сканує наданий IP-адреса з інтенсивним скануванням і відображає результат сканування нижче вкладки Output Zenmap.
5. Після завершення сканування, Zenmap показує результат сканування. Перейдіть на вкладку Port/Hosts для відображення додаткової інформації про результати перевірки.
6. Zenmap також відображає порт, протокол, статус, службу і версію сканування.
7. Перейдіть на вкладку Topology для перегляду топології Zenmap для наданої IP-адреси в інтенсивному профілі сканування.

Висновки та результати роботи

За результатами роботи необхідно надати звіт про всі проведені сканування та надати аналіз обробленої інформації.

Надати рекомендації для зменшення ризику витоку критичної інформації для мережі через отримані при скануванні дані.

Звіт оформити в формі звіту керівнику організації з підтвердженнями знайденої критичної інформації та рекомендаціями для вдосконалення захисту мережі.

Лабораторна робота №6 «Вирішення проблем мережі з використанням інструменту MegaPing»

MegaPing є кінцевим інструментарієм, який надає повний спектр необхідних утиліт та інформації системного адміністратора і постачальників IT-рішень.

Будь-які компанії, що існують в Інтернеті, вимагають веб-серверів. Атакуючий зазвичай використовує сервер WWW під керуванням IIS і командного рядка і отримує доступ до системи. Цей процес прослуховує порт 80 хоста WWW і перенаправляє трафік. Процес захоплює трафік в HTTP заголовках і направляє його в WWW сервера порт 80, після чого зловмисник намагається увійти в систему; коли доступ отримано, встановлює додаткові інструменти для подальшого використання мережі.

MegaPing сканера безпеки перевіряє вашу мережу для потенційних вразливостей, які можуть бути використані для атаки мережі, а також зберігає інформацію в звітах безпеки. В цій роботі ви навчитеся використовувати MegaPing, щоб перевірити наявність вразливостей і усунення неполадок.

Проблематика, завдання та цілі виконання лабораторної роботи

Ця робота дає уявлення про пінгування адреси призначення. Необхідно виконати:

- Пінг адресатів адресу
- Трасування
- Виконайте сканування NetBIOS

Щоб виконати лабораторну, вам необхідно:

- Ви також можете завантажити останню версію MegaPing за посиланням http://www.magnetosoft.com
- Адміністративні привілеї для запуску інструментів
- Параметри TCP / IP налаштований правильно і доступний сервер DNS
- Ця лабораторія буде працювати на Windows Server 2012, Windows 2008 і Windows 7

Практичні рекомендації для виконання

1. Виберіть IP-сканер, і тип в діапазоні IP; в цій лабораторній роботі діапазоні IP від 192.168.1.1 до 192.168.1.254 натисніть кнопку Пуск
2. Сканування портів
3. Ви можете вибрати діапазон IP в залежності від мережі.

4. Використання Whois.
5. Потім правою кнопкою миші і виберіть опцію Traceroute.
6. Він відкриється вікно Traceroute, і простежимо зворотні IP адреса.

Документуйте всі IP-адреси, відкриті порти і їх запущені додатки та протоколи, виявлені в ході виконання лабораторної.

Висновки та результати роботи

За результатами сканування надати:

- Список активних хостів
- NetBios Name
- Adapter Name

У висновках проаналізуйте інструменти, що використовувались у всіх наведених завданнях, дайте аналіз користі для Вас, як «білого хакеру» та надайте звіт по вибраній організації, яку Ви взяли на аналіз.

Для аналізу Ви можете використовувати різноманітні інструменти зі схожими характеристиками для більш повного аналізу вразливостей компанії.

З використанням інструменту MegaPing надайте звіт безпеки компанії.

Лабораторна робота №7 «Віруси в мережі та на окремих хостах. Використання інструменту ProRat Tool для дослідження вірусів»

ProRat — це бекдор-троян на базі Microsoft Windows, більш відомий як інструмент віддаленого адміністрування. Як і інші трояни, він використовує клієнт і сервер. ProRat відкриває порт на комп'ютері, який дозволяє клієнту виконувати численні операції на сервері (машині, якою керують). ProRat доступний у безкоштовній та платній версіях. У безкоштовній версії ProRat не може підключатися до користувачів через глобальні мережі (WAN), лише через локальні мережі (LAN). ProRat відомий тим, що його сервер майже неможливо видалити без оновленого антивірусного програмного забезпечення.

Проблематика, завдання та цілі виконання лабораторної роботи

Троянська програма, яка містить шкідливий код всередині виглядають нешкідливими програмами, таким чином вони можуть отримати контроль над системою і привести до шкоди, наприклад, руйнуючи таблицю розміщення файлів на жорсткому диску.

Мета цієї лабораторії, щоб допомогти студентам навчитися виявляти троянські та бекдор атаки.

Огляд троянів і бекдорів

За допомогою трояна, зловмисник отримує доступ до збережених паролів в комп'ютері і буде мати можливість читати особисті документи, видаляти файли, показувати картинки, і / або показувати повідомлення на екрані.

Практичні рекомендації для виконання

Створення сервера за допомогою ProRat Tool

1. Відкрийте ProRat і натисніть кнопку Створити Pro Rat Server, щоб почати підготовку до створення сервера
2. Відкриється вікно Створення сервера
3. Натисніть Загальні настройки для зміни функцій, таких як порт сервера. Пароль сервера жертви, Ім'я та номер порту.
4. Зніміть виділені параметри, як показано на наступному скріншоті.
5. Натисніть Bind Файл, щоб зв'язати сервер з файлом;
6. Виберіть файл для зв'язування з сервером.
7. Виберіть файл у вікні, а потім натисніть кнопку Відкрити, щоб зв'язати файл.
8. В налаштуваннях сервера Розширення, виберіть EXE (підтримує значок) в настройках Виберіть розширення сервера.

9. В іконі сервера виберіть будь-який із значків, і натисніть на кнопку Створити сервер в нижній правій частині вікна ProRat
10. Тепер ви можете відправити файл сервера поштою або будь-яким середовищем передачі даних на комп'ютер жертви.
11. Відкрийте binder_server.exe
12. Тепер перейдіть в Windows 8 Virtual Machine і введіть IP-адресу Windows Server 2008 і живий номер порту за замовчуванням в головному вікні ProRat і натисніть Connect.
13. У цій лабораторній IP-адреса Windows Server 2008
14. Введіть пароль, який ви вказали під час створення сервера і натисніть кнопку OK
15. Тепер ви підключені до зараженого комп'ютера. Щоб перевірити підключення, натисніть PC Info і виберіть системну інформацію
16. Тепер натисніть KeyLogger для крадіжки паролів користувачів в системі онлайн
17. Вікно Key Logger з'явиться.
18. Тепер перейдіть на Windows Server 2008 машини і відкрити браузер або Блокнот і введіть будь-який текст
19. У той час як жертва пише повідомлення або вводить ім’я користувача і пароль, ви можете перехопити їх.
20. Тепер перейдіть на Windows 8 Virtual Machine і натисніть Read та час від часу перевіряйте наявність оновлень даних з зараженого комп'ютера.
21. Тепер ви можете використовувати безліч функцій з ProRat на машині жертви.

Висновки та результати роботи

Проаналізуйте отримані дані та надайте звіт про проведені роботи. Проаналізуйте можливості використання даного програмного забезпечення в зловмисних цілях. Надайте розгорнутий звіт з результатами лабораторної роботи.

Лабораторна робота №8 «Створення та аналіз вірусів з використанням інструментів OneFileEXEMaker та Atelier Web Remote Commander»

Комп’ютерні віруси це вид шкідливого програмного забезпечення, яке здатне поширювати свої копії з метою інфікування та пошкодження даних на пристрої жертви. Віруси можуть потрапити на комп’ютер з інших вже інфікованих пристроїв, через носії інформації (CD, DVD тощо) або через Інтернет-мережу.

Проблематика, завдання та цілі виконання лабораторної роботи

Чи не найбільше атак на мережі спричинено вірусами. Не знаючи принципів кібергігієни можна «заразитись» комп’ютерним вірусом та «покласти» всю мережу. Це призведе до катастрофічних наслідків для компанії.

В роботі системного адміністратора велику увагу відведено наданню співробітникам компанії пам’яток та рекомендацій для зменшення імовірності проникнення різноманітного зловмисного програмного забезпечення.

В даній лабораторній роботі на прикладі створення вірусів вивчатимемо його будову та впровадження в систему різноманітними шляхами з використанням інструментів OneFileEXEMaker та Atelier Web Remote Commander. За бажання можна використовувати інше програмне забезпечення зі схожими інструментами та призначенням.

Практичні рекомендації для виконання

Створення трояна за допомогою OneFileEXEMaker

1. Встановіть OneFileEXEMaker на Windows Server 2008 Virtual Machine
2. Натисніть на кнопку Add File і виберіть два файли і додати їх.
3. Виберіть Mcafee і введіть 8080 в поле Параметри командного рядка
4. Виберіть Лазаріс і перевірте нормальний варіант у відкритому режимі
5. Натисніть кнопку Зберегти і переглянути, щоб файл зберігся на робочому столі, і ім'я файлу Tetris.exe
6. Тепер двічі клацніть, щоб відкрити файл Tetris.exe
7. Тепер відкрийте диспетчер задач і відкрийте вкладку Процеси, щоб перевірити його. McAfee працює.

Трояни віддаленого доступу за допомогою Atelier Web Remote Commander

1. Установка і запуск Atelier Web Remote Commander (AWRC) в Windows Server 2012
2. Відкрийте головне вікно додатку

3. Введіть IP-адресу і Ім'я користувача / пароль віддаленого комп'ютера.
4. Натисніть кнопку Connect, щоб отримати доступ до машини віддалено
5. Commander підключений до віддаленої системи. Перейдіть на вкладку Sys Info, щоб переглянути повну інформацію про віртуальній машині
6. Виберіть Networklnfo шлях, де ви можете переглядати інформацію про мережі
7. Виберіть користувачів і групи, які будуть відображати повну інформацію про користувача

Висновки та результати роботи

У висновках надайте звіт по вірусним атакам, що вдались, надайте скріншоти успішно заражених хостів (пам’ятайте про Законодавство України).

За результатами роботи надайте перелік вимог для уникнення можливостей реалізації даних атак.

Роботу оформіть як звіт керівнику організації з списком вимог та рекомендацій для протидії схожих атак в майбутньому.

СПИСОК ДЖЕРЕЛ ІНФОРМАЦІЇ:

1. Конституція України
2. Закон України «Про інформацію»
3. Закон України «Про Державну таємницю»
4. Закон України «Про основи Національної безпеки України»
5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»
6. http://www.advanced-ip-scanner.com
7. http: / / www.nirsoft.net/utils/cports.html
8. http://nmap.org
9. http://www.magnetosoft.com

ДЛЯ НОТАТОК

Навчально-методичне видання

ТЕХНОЛОГІЇ СТВОРЕННЯ ТА ЗАСТОСУВАННЯ СИСТЕМ ЗАХИСТУ ІНФОРМАЦІЇ

Методичні вказівки
до виконання лабораторних робіт
для студентів спеціальностей 123 «Комп'ютерна інженерія»
та 125 «Кібербезпека»

Укладачі: **КОНДАКОВА** Світлана Віталіївна;
КОНДАКОВА Анастасія Михайлівна

Комп'ютерне верстання *М.М. Власенко*

Підписано до друку 02.02.2023 Формат 60 х 84 1/ 16
Ум. друк. арк. 1,86. Обл.-вид. арк. 1,14.
Електронний документ. Вид № 59/ІІІ-17.

Видавець і виготовлювач
Київський національний університет будівництва і архітектури

Повітрофлотський проспект, 31, Київ, Україна, 03680
Свідоцтво про внесення до Державного реєстру суб'єктів
видавничої справи ДК № 808 від 13.02.2002 р.