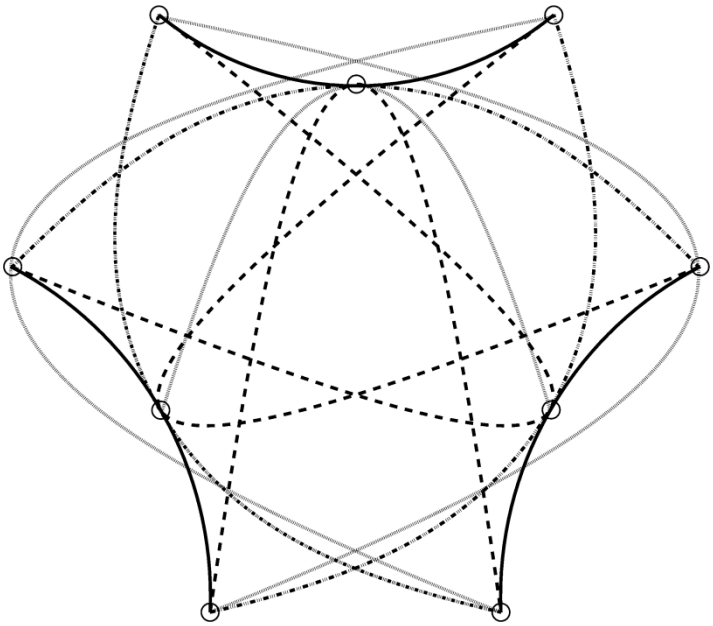
МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

ТЕРНОПІЛЬСЬКИЙ НАЦІОНАЛЬНИЙ ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

КАФЕДРА КІБЕРБЕЗПЕКИ

ОПОРНИЙ КОНСПЕКТ ЛЕКЦІЙ
з дисципліни
«МОНІТОРИНГ МЕРЕЖЕВОЇ БЕЗПЕКИ»
для студентів спеціальності “Кібербезпека”
освітнього рівня “магістр”



ТЕРНОПІЛЬ -2019

Опорний конспект лекцій з дисципліни “Моніторинг мережевої безпеки” для студентів напряму підготовки “кібербезпека” освітнього рівня “магістр”/ Тернопільський національний економічний університет; Уклад. В.В. Яцків, І.З. Якименко–Тернопіль,ФО-П Шпак В., 2019. – 68 с.

Опорний конспект лекцій складаються з частин, що рекомендовані програмою на основі освітньо-професійної програми підготовки магістра галузі знань 12 Інформаційні технології спеціальності – 125 Кібербезпека

Укладачі: Яцків Василь Васильович, д.т.н., доцент
Якименко Ігор Зіновійович, к.т.н., доцент,

Рецензенти: Шевчук Р.П., к.т.н., доцент, доцент кафедри комп’ютерних наук Тернопільського національного економічного університету;
Кінах Я.І, к.т.н., доцент кафедри програмної інженерії Тернопільського національного технічного університету ім. І.Пулюя.

Затверджено на засіданні кафедри кібербезпеки
протокол №3 від 29.10.2019.

Розглянуто та схвалено групою забезпечення з кібербезпеки
протокол №2 від 29.10.2019.

Розглянуто та схвалено вченою радою факультету комп’ютерних інформаційних технологій, протокол №__ від _____2019 р.

ЗМІСТ

Передмова

В даний час діяльність багатьох організацій залежить від стану їх інформаційних систем. При цьому інфраструктура інформаційних систем часто містить вузли та системи, порушення безпеки яких може привести до нанесення значного збитку для ведення бізнесу в організації.

Для запобігання таких випадків, як правило, після відповідного аналізу формується перелік актуальних загроз і розробляється комплекс заходів щодо їх нейтралізації. В кінцевому підсумку будується система управління інформаційною безпекою, яка включає в себе різні засоби захисту, що реалізують необхідні захисні механізми. До складу даної системи може входити підсистема управління вразливими, що представляє собою комплекс організаційно-технічних заходів, спрямованих на запобігання використання відомих вразливостей, потенційно існуючих в системі, що захищається або в мережі. Зокрема, в рамках управління вразливостями проводяться такі заходи, як періодичний моніторинг захищеності інформаційних систем і усунення виявлених вразливостей.

Останнім часом велика увага приділяється новому напрямку в області захисту інформації - адаптивної безпеки комп'ютерної мережі. Цей напрямок включає в себе дві основні технології: аналіз захищеності (SecurityAssessment) і виявлення атак (IntrusionDetection). Метою даного навчального посібника є ознайомлення студентів з теоретичними питаннями, пов'язаними з архітектурою і принципами роботи систем виявлення атак зловмисників, а також прийомами та інструментами, застосовуваними при захисті комп'ютерних систем і мереж від атак.

Посібник призначений для студентів, які навчаються за напрямом підготовки «Інформаційна безпека» (комплексне забезпечення інформаційної безпеки автоматизованих систем - КОІБАС, організація і технологія захисту інформації і т. Д.), І слухачів факультету підвищення кваліфікації за цим напрямком. Може представляти інтерес для студентів і аспірантів інших спеціальностей, що займаються питаннями використання сучасних засобів і методів забезпечення інформаційної безпеки комп'ютерних систем.

В рамках даного навчального посібника розглядаються наступні теми:

- необхідність і актуальність розробки та впровадження технологій виявлення і запобігання атак (IDS/IPS);
- зрозумілий апарат в області моніторингу інформаційної безпеки в частині виявлення та запобігання вторгнень;
- архітектура системи IDS / IPS (джерела даних, ознаки атак, методи виявлення атак, механізми реагування);
- спеціалізовані технології IDS/IPS;
- централізоване управління мережевими і хостовими технологіями IDS / IPS різних виробників і їх взаємодію з іншими механізмами захисту;
- огляд і напрямку розвитку перспективних IDS/IPS. Пропонований матеріал може бути використаний при вивченні наступних дисциплін: методи і

засоби забезпечення інформаційної безпеки, технологія захисту комп'ютерних систем, програмно-апаратні засоби захисту інформації, аудит інформаційної безпеки, моніторинг інформаційних систем і т. д.

Засвоєння матеріалу, наведеного в навчальному посібнику, дозволить студентам застосовувати отримані знання в області моніторингу та управління інформаційною безпекою та технологій виявлення атак, розпізнавати ознаки атак, оперувати джерелами даних для IDS / IPS, використовувати методи виявлення атак, методи збору інформації про мережу, механізми реагування і спеціалізовані системи для виявлення і запобігання атак на комп'ютерні системи управління і методи їх відновлення, а також мати навички ідентифікації мережевих об'єктів, визначення топології мережі, ідентифікації статусу порту, сервісів і додатків, операційних систем, централізованого управління уразливими, централізованого управління технологіями IDS / IPS і організації їх взаємодії з іншими механізмами захисту інформаційних мереж.

Позначки використовувані в книзі

У книзі використовуються наступні піктограми для позначення мережевих пристроїв різних типів:

Тема 1. ПОСТАНОВКА ЗАДАЧІ АНАЛІЗУ ЗАХИЩЕНОСТІ КОМП'ЮТЕРНОЇ СИСТЕМИ

1.1. Корпоративна мережа як об'єкт захисту

Головне завдання корпоративної мережі - централізоване управління підприємством або об'єднанням підприємств. Мережа забезпечує передачу інформації між різними додатками, використовуваними в даній організації. Взаємодіючі додатки можуть бути розташовані в різних філіях організації, територіально віддалених один від іншого і з'єднаних між собою виділеними каналами зв'язку. Обмін інформацією здійснюється за допомогою глобальної мережі Інтернет.

Типова конфігурація корпоративної мережі представлена на рис. 1.1.

Для захисту комп'ютерних систем від неправомірного втручання в процеси їх функціонування і несанкціонованого доступу (НСД) до інформації використовуються різні захисні механізми, наприклад: йдуть Франція, Італія і Німеччина, що узгоджується із загальною картиною поширеності цих систем. Необхідно відзначити, що в компонентах, найбільш використовуваних в мережі Інтернет, вразливостей виявлено мало. В цілому уразливими виявилися більш 10% доступних АСУ ТП (див. рис. 1.26, рис. 1.27).

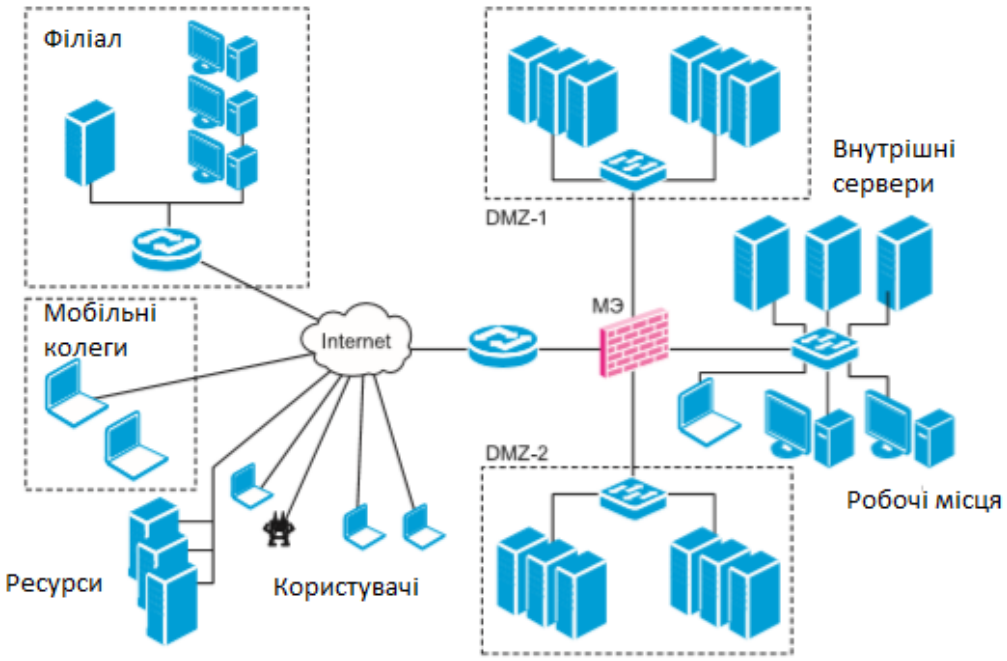


Рис. 1.1. Типова конфігурація корпоративної мережі (МЕ - міжмережевий екран)

Контрольні питання

1. Яка мета захисту корпоративної інформаційної системи?
2. Назвіть захисні механізми. Як їх можна класифікувати?
3. Дайте визначення поняттям «загроза інформаційній безпеці», «вразливість» і «атака». Опишіть взаємозв'язок між ними.
4. Перерахуйте основні класифікаційні схеми вразливостей. Які їх основні переваги та недоліки?
5. Назвіть основні джерела інформації про уразливість. Яка із загальнодоступних баз даних про уразливість більш краща?

Тема 2. МЕТОДИ ВИЯВЛЕННЯ ВРАЗЛИИИХ І СИСТЕМИ АНАЛІЗУ ЗАХИЩЕНОСТІ

2.1. Основні прийоми виявлення вразливостей

Як зазначалося вище, причинами виникнення вразливостей є помилки проектування, реалізації та експлуатації. Нижче наведені методи виявлення таких помилок.

Аналіз алгоритму програмно-апаратного забезпечення.

Даний метод використовується в основному для пошуку вразливостей проектування. При- мером практичної реалізації може служити система PVS (Prototype Verification System), розроблена в Computers Science Laboratory інституту SRI (http://pvs.csl.sri.com/).

На практиці часто виконується пошук помилок реалізації (коду), що здійснюються за допомогою таких методів.

Динамічний аналіз безпеки програми.

Одним з найбільш простих і поширених при пошуку вразливостей реалізації є DAST (Dynamic Application Security Testing) - динамічний (т. Е. Що вимагає виконання) аналіз безпеки додатки без доступу до вихідного коду і середовищі виконання серверної частини. Іншими словами, аналіз додатки методом «чорного ящика»..

У цьому контексті досить часто використовується термін «фаззінга» (fuzz testing, fuzzing). Даний метод передбачає вивчення поведінки ПО за допомогою подачі на вхід різних значень змінних. Найчастіше це граничні або малоймовірні значення, які можуть створити умови, що призводять до переповнення буфера, виходу за межі масивів, записи в неприпустимі області пам'яті і т. д.

Закінчення табл. 2.1

Вендор	Склад рішення	Джерело
Symantec	Symantec™ Control Compliance Suite Standards Manager Symantec Control Compliance Suite Vulnerability Manager (CCS VM)	http://www.symantec.com/page.jsp?id=control-compliance-suite
Assuria	Assuria Auditor	http://www.assuria.com
АЛТЭКС-СОФТ	RedCheck	http://www.redcheck.ru/
GFI	LANguard	http://www.gfi.ru/ languard
Rapid7	Nexpose Metasploit	http://www.rapid7.com/products/nexpose/

Контрольні питання

1. Перерахуйте методи виявлення вразливостей, що виникли на етапах проектування, програмування і експлуатації
2. Охарактеризуйте динамічний і статичний аналіз безпеки програми. У чому їх принципова різниця?
3. Перерахуйте три способи перевірки систем на наявність вразливостей.
4. Охарактеризуйте достоїнства і недоліки мережевих, локальних і пасивних агентів сканування.

Тема 3. МЕРЕЖЕВІ СКАНЕРИ БЕЗПЕКИ

3.1 Розміщення мережевих агентів сканування в мережі

В даний час найбільш використовуваними є сканери (скануючі модулі), що виконують перевірки дистанційно. Розглянемо їх можливості більш детально.

Для виконання перевірок агентам даного типу необхідно мережеве взаємодія з об'єктами сканування. Це обумовлює такі особливості:

- тривалість сканування;
- вплив засобів захисту;
- створеня навантаження на мережу.

Для виявлення вразливостей мережеві агенти застосовують різні способи. Вище вже згадувалися два способи виявлення вразливостей: тести і логічні висновки. Мережеві агенти мають наступні категорії перевірок:

- банерні перевірки;
- підбір облікових засобів;
- системні (локольні) перевірки;
- експлойти.

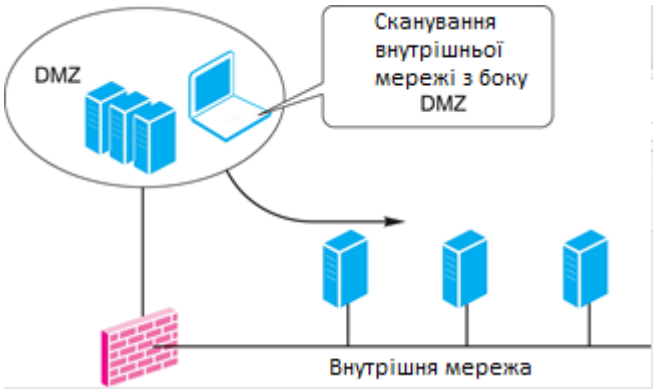


Рис. 3.5. Оцінка захищеності внутрішньої мережі порушником з DMZ

Таким чином, вибір варіанту розміщення мережевих агентів проводиться, виходячи з необхідності моделювання дій потенційного порушника або для зняття обмежень, пов'язаних з фільтрацією трафіку.

3.2. Мережеві агенти і збір інформації

Мережеві агенти підключаються до об'єкту сканування вузлів віддалено, при цьому за допомогою одного агента перевіряється велика кількість вузлів мережі. Тому важливою функціональною складовою мережевого агента є модуль збору інформації, що виконує так звані інвентаризаційні перевірки.

Инвентаризационная информация необходима для работы некоторых категорий проверок, например баннерных. Кроме того, наличие подробной информации об объектах сканирования может помочь в принятии решения об устранении найденных уязвимостей. В целом сетевой сканер выполняет следующие инвентаризационные проверки:

- ідентифікацію пристроїв мережі;
- визначення топології, взаємного розташування вузлів;
- ідентифікаціювідкритих портів;
- ідентифікаціюмереж;
- ідентифікаціюдодатків;
- ідентифікаціюопераційних систем.

Контрольні питання

1. Які категорії перевірок мають мережеві агенти?
2. Перерахуйте можливі варіанти розміщення мережевих скануючих модулів.
3. З чим пов'язаний вибір варіанта розміщення мережевих агентів?
4. Які інвентаризаційні перевірки виконує мережевий сканер?

Тема 4. СПОСОБИ ЗБИРАННЯ ІНФОРМАЦІЇ ПРО МЕРЕЖУ. ПОПЕРЕДНЄ ВИВЧЕННЯ ЦІЛІ

4.1. Способи збору інформації про мережу

У процесі дистанційного контролю стану захищеності виникає необхідність збору інформації про мережеві об'єктах. В залежності від варіанту контролю захищеності, обраної методології і інших чинників можуть бути використані різні прийоми збору інформації. Наприклад, при виконанні аудиту внутрішньої мережі на відповідність вимогам політики безпеки звичайно не потрібно визначати топологію мережі або збирати інформацію реєстраційного характеру. Усе це вже, як правило, відомо. Крім того, оцінці захищеності периметра зазвичай передує етап попереднього вивчення мети, що передбачає збір інформації «з нуля».

Способи збору інформації про систему можна розділити на дві групи (рис. 4.1):

- активні(Activefingerprinting), які передбачають використання ключових впливів на систему і аналіз відгуків;
- пассивні(Passivefingerprinting), які передбачають використання інформації, «добровільно» розсилається досліджуваної системою.

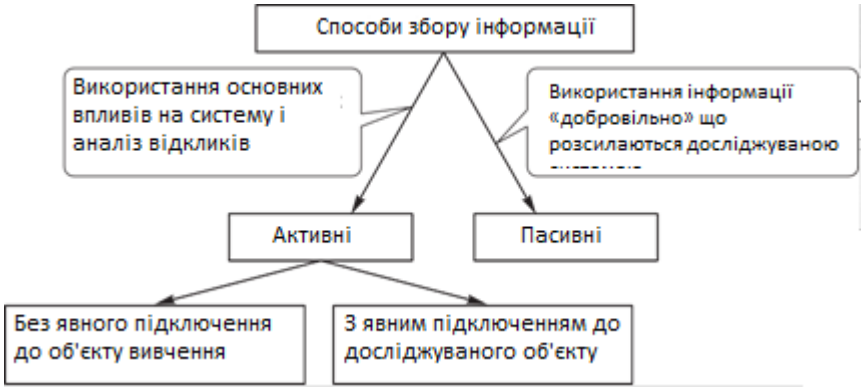
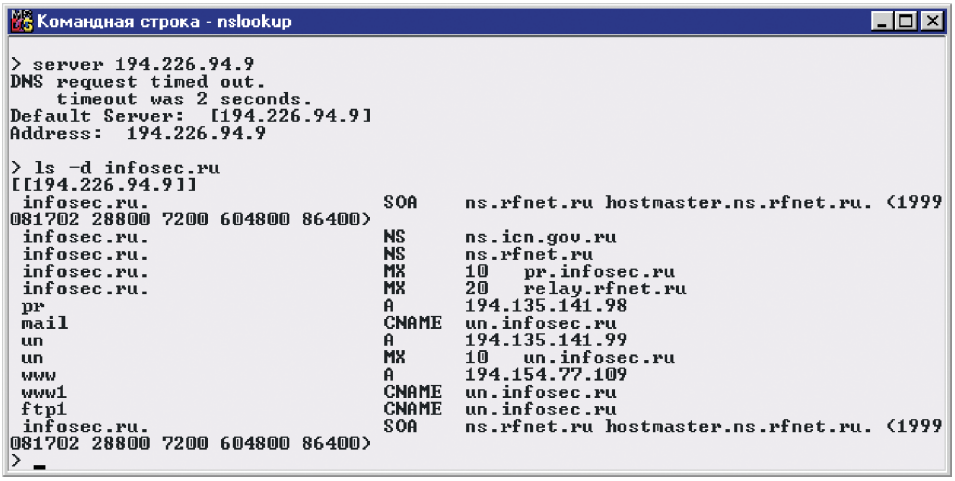


Рис. 4.1. Способи збору інформації про мережу

Активні методи збору інформації в свою чергу можна розділити на що вимагають явного підключення до мережних служб об'єкту сканування (наприклад, ідентифікація сервісів за допомогою посилки різних запитів) і не потребують такого підключення. Остання група методів називається також попереднє вивчення мети.

В ході збору інформації про систему можуть бути отримані різні відомості, наприклад:

- інформація реєстраційного та організаційного характеру, зазвичай доступна



через Інтернет;

Рис. 4.7. Збір інформації реєстраційного характеру за допомогою утиліти nslookup

Мета даного етапу - отримання списку вузлів, що належать домену, і отримання відповідностей «IP-адреса / ім'я». На основі даного списку може бути отриманий діапазон адрес, що належать організації. На додаток до запитів до бази тут також можна використовувати кілька технік:

- деякі адреси / імена зобов'язані існувати просто для того, щоб домен працював. Це, наприклад, сервер (и) імен (NS) і поштові сервери (MX). Адреса сервера імен можна отримати з інформації реєстраційного характеру, а адреса поштового сервера - з бази сервера імен;
- деякі адреси / імена з великим ступенем ймовірності будуть присутні в домені, наприклад, www, mail, gate, firewall. Необхідно перевірити існування вузлів з такими іменами;
- як правило, вузли належать однієї підмережі, тому, отримавши одну адресу, слід перевірити і інші адреси підмережі;
- використання бази даних сервера імен (передача зони).

Слід враховувати, що прямий DNS-запит (Ім'я IP-адреса) і зворотний (IP-адреса Ім'я) не завжди дають порівнянні результати.

Основними результатами попереднього вивчення мети слід вважати:

- список доменів, що мають відношення до досліджуваної організації;
- діапазони адрес для подальшого дослідження;
- іншу інформацію, зібрану при дослідженні мети.

Ця інформація може бути використана в якості вихідної для збору відомостей іншими методами.

Контрольні питання

1. Охарактеризуйте способи збору інформації про систему.
2. Які відомості можуть бути отримані вході збору інформації про систему?
3. Перелічіть і охарактеризуйте прийоми попереднього вивчення мети.

Тема 5. ІДЕНТИФІКАЦІЯ МЕРЕЖЕВИХ ОБ'ЄКТІВ

Тема 4 була присвячена методам збору інформації без явного підключення до об'єкта дослідження.

Розглянемо прийоми, які передбачають явне підключення при ідентифікації:

- мережевих об'єктів;
- статусу порту;
- сервісів;
- додатків;
- операційних систем.

Завдання ідентифікації мережевих пристроїв полягає в тому, щоб віддалена система відреагувала на який-небудь запит (рис. 5.1).

Під реакцією системи розуміється генерація якої-небудь відповіді або повідомлення про помилку. Це і буде доказом того, що система присутня в мережі. Причому завдання полягає саме в доказі знаходження системи, а не в конкретних яких-небудь її характеристик

Рис. 5.1 Реакція системи на запит

(Працюючі служби, ОС і т. П.). Для вирішення цього завдання можна використовувати різні протоколи: IP, ICMP, UDP, TCP.

5.1. Використання протоколу ICMP

Загальні відомості про протокол ICMP. Протокол ICMP (RFC792) служить для виявлення проблем, пов'язаних з мережевим рівнем (в стеку TCP / IP цей рівень представлений протоколом IP). Повідомлення протоколу ICMP передаються у вигляді IP-датаграм, т. Е. До них додається заголовок IP. Формат ICMP-пакета представлений на рис. 5.2.

Type (тип)	Code (код)	Checksum (Контрольна сума)
Дані…		

Рис. 5.2. Формат ICMP-пакета

Існує кілька типів повідомлень ICMP. Кожен тип повідомлення має свій формат, при цьому всі вони починаються з наведених в табл. 5.1 трьох полів:

- 8-бітного цілого числа, що позначає тип повідомлення (TYPE);
- 8-бітного поля коду (CODE), який конкретизує призначення повідомлення;
- 16-бітного поля контрольної суми (CHECKSUM).

Контрольні питання

1. У чому полягає завдання ідентифікації мережевих пристроїв?
2. Як за допомогою посилки ARP-запитів можна виявити вузли мережі?
3. Як використовуються ICMP-повідомлення про помилки для виявлення пристроїв?
4. Якими способами може бути виконана ідентифікація мережевих пристроїв за допомогою протоколу ICMP?

Тема 6. ВИЗНАЧЕННЯ ТОПОЛОГІЇ МЕРЕЖІ

Із завданням ідентифікації мережевих об'єктів пов'язана задача побудови топології (карти) сканируемой мережі. Часто (наприклад, при скануванні внутрішньої мережі) топологія відома заздалегідь, але в деяких випадках топологію необхідно спеціально досліджувати.

6.1. Відстеження маршрутів

Загальні відомості. При визначенні топології мережі (на етапі початкового збору відомостей) поширеним прийомом є відстеження маршрутів. Для цього використовується утиліта traceroute, що входить до складу систем UNIX (в Windows вона називається tracert). Мета такого дослідження - отримати точний маршрут руху IP-пакета від одного вузла мережі до іншого.

Розглянемо роботу утиліти tracert зі складу Windows на наступному прикладі.

Нехай команда tracert виконується щодо вузла 200.2.2.222:

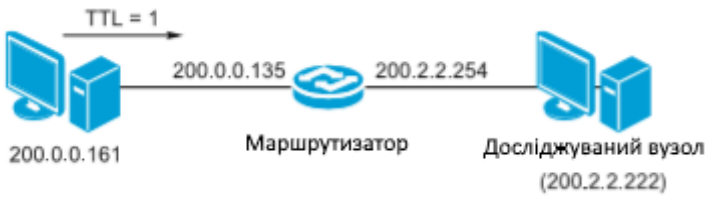
>tracert 200.2.2.222 –d:

1. На першому кроці надсилається ICMP-запит (Echo) з наступними параметрами:

адрес відправника —100.0.0.161;

адрес отримувача — 200.2.2.222;

TTL=1.



start_destination_port = (53 — (num_of_hopes*num_of_probes)) – 1, де 53 – порт дозволеного протоколу DNS.

6.2 Відстежування маршрутів і фільтрація

Однак наступний пакет матиме вже інше значення порту одержувача і буде блокований. Тому бажано, щоб значення порту одержувача було постійним. Це може бути досягнуто установкою виправлення до утиліти traceroute (до версії 1.4a5). Її синтаксис після застосування виправлення має вигляд

traceroute -S —p53 200.0.0.222

6.3. Утиліта traceproto

Роблячи висновок щодо застосування утиліти traceroute, можна сказати, що вона працює на мережевому рівні (IP), проте в умовах фільтрації трафіку її застосування обмежене транспортним рівнем (тим, що дозволено з верхніх протоколів - UDP, ICMP, TCP). Тому за допомогою утиліта traceroute можна визначити останній шлюз, від якого надійшла відповідь. З точки зору відстеження маршрутів важливим є значення поля TTL з заголовка IP, але не більше того. Протоколи UDP і ICMP лише транспортують дані, тому без шкоди можуть бути замінені будь-яким іншим протоколом транспортного рівня, зокрема TCP.

Ця ідея реалізована в утиліті traceproto(http://traceproto.sourceforge.net/index.php).

Утиліта traceproto аналогічна утиліті traceroute, але дозволяє використовувати також і протокол TCP для відстеження маршрутів.

Синтаксис утиліти traceproto:

traceproto [-cCfhv] [-p protocol] [-d dst_port] [-D max_dst_port] [-s src_port] [-S max_src_port] [-m min_ttl] [-M max_ttl] [-w response_timout] [-W send_delay] [-a account_level] [-P payload_size] [-k skips] [-H packets_ per_hop] [-i incr_pattern] [-o output_style]

Видно, що протокол вибирається за допомогою опції -p (за замовчуванням TCP), порт одержувача задається опцією -d (за замовчуванням 80), зрозуміло, можна задати і порт джерела. Про призначення інших опцій можна дізнатися з керівництва до утиліти.

Контрольні питання

1. Опишіть прийом «відстеження маршрутів» при визначенні топології мережі.
2. У чому полягає специфіка завдання відстеження маршрутів при наявності пристроїв, що здійснюють фільтрацію трафіку?
3. Яке призначення утиліти traceproto?

Тема 7. ІДЕНТИФІКАЦІЯ СТАТУСУ ПОРТУ

7.1. Сканування портів

Взаємодія вузлів по протоколам TCP і UDP передбачає використання портів для ідентифікації додатків. Отже, визначивши номера відкритих портів на віддаленому вузлі, можна в подальшому дізнатися про працюючих на ньому додатках, зробити висновок про роль цього вузла в корпоративній мережі, дізнатися версію ОС. Визначити стан портів на віддаленому вузлі можна, наприклад, послідовним перебором. Цей процес зазвичай називають скануванням портів (рис. 7.1).

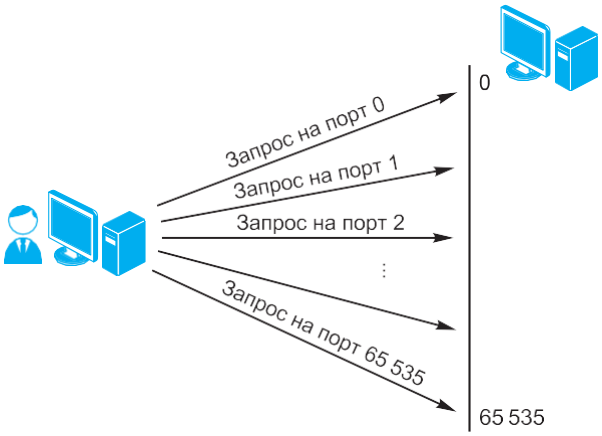


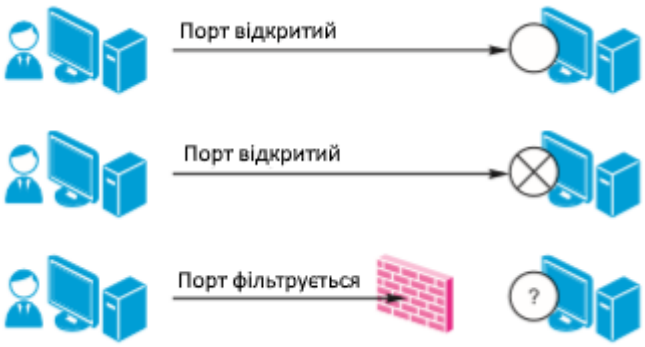
Рис. 7.1. Процессканування портів

Фактично порт на віддаленому вузлі може перебувати в одному з двох станів: відкритий, закритий.

7.2 Сканування портів TCP

Але при віддаленому підключенні внаслідок впливу міжмережевий екран не завжди можна точно дізнатися статус порту. В цьому випадку зазвичай вказується, що порт фільтрується (рис. 7.2).

Завдання ідентифікації статусу порту можна вирішувати кількома способами.



Розглянемо деякі з них.

Рис. 7.2. Визначення статусу порту при віддаленому підключенні

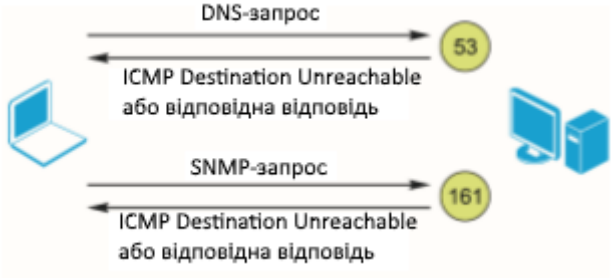


Рис. 7.13. «Обдумані» запити до сервісів

Контрольні питання

1. У чому полягає завдання ідентифікації статусу порту?
2. Опишіть особливості сканування TCP-портів.
3. У чому відмінність TCP-сканування від сканування UDP-портів?

Тема 8. ІДЕНТИФІКАЦІЯ СЕРВІСІВ І ДОДАТКІВ

8.1. Ідентифікація TCP-служб

Завдання ідентифікації служб (додатків) - найважливіша в контексті аналізу захищеності. Значна частина вразливостей відноситься до рівня додатків. На основі інформації, зібраної на даному етапі, будуються методи виявлення вразливостей за непрямими ознаками.

Використання банерів. «Класичний »метод збору інформації про запущеної на сканованому вузлі службі - аналіз банерів. Цей метод полягає в аналізі вітань, виведених службами при підключенні на заданий порт. Часто банери містять інформацію про використовувану службі, аж до номера версії. Оскільки не всі служби є абсолютно переносяться, це дає можливість робити припущення про використовувану ОС, наприклад:

telnet ftp.dmn1.ru 21
220 telnetftp.dmn1.ruFTPserver (Versionwu-2.4(37) MonFeb 15 16:48:38 MSK 1999) ready.

telnet smtp.dmn1.ru 25
220 smtp.dmn1.ru ESMTP Sendmail 8.11.2/8.11.2; Thu, 21 Jun 2001 18:34:19 +0400
…

При цьому слід зазначити такі недоліки:

• багато служб дозволяють адміністратору довільно редагувати свої вітання, т. Е. Існує ймовірність (хоча і досить мала), що служба не та, за кого себе видає;

з метою визначення підтримуваних ними типів IP.

Отримана інформація може бути використана для попереднього налаштування модуля стеження системи виявлення атак.

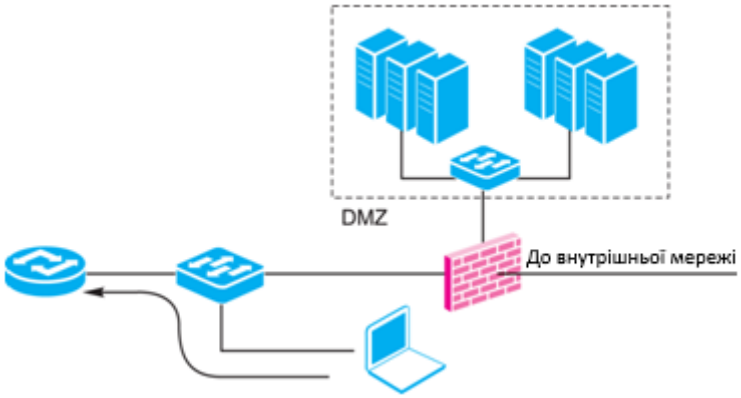


Рис. 8.1. Модуль стеження IDS між маршрутизатором і між мережевим екраном

Принцип сканування полягає в наступному (рис. 8.2).

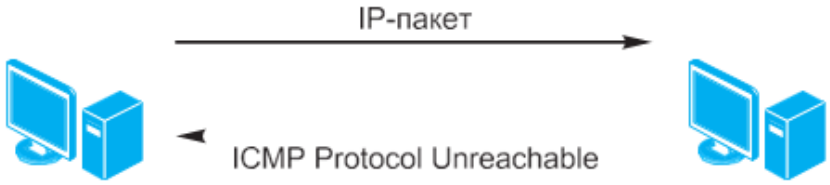


Рис. 8.2. Сканування протоколів

На вузол посилається IP-пакет з необхідним значенням поля «тип протоколу» в заголовку.

Якщо у відповідь прийшло повідомлення ICMP Protocol Unreachable, протокол не підтримується. Якщо відповідь не прийшла, протокол підтримується. Цей тип сканування дуже нагадує UDP-сканування, тому йому притаманні ті ж проблеми. Наприклад, при скануванні міжмережевих екранів пакет ICMP Protocol Unreachable може бути заблокований, і тоді можливо велике число помилкових спрацьовувань.

Для проведення сканування можна використовувати сканер nmap. синтаксис:

nmap —sO<сканований вузол >

Контрольні питання

1. У чому полягає суть методу аналізу банерів?
2. Перерахуйте методи, засновані на аналізі особливостей роботи служб. Які їх переваги в порівнянні з методом аналізу банерів?
3. Дайте характеристику і приведіть особливості роботи утиліти nmap.
4. Як проводиться ідентифікація UDP-служб?
5. У чому полягає метод сканування протоколів?

Тема 9. ІДЕНТИФИКАЦІЯ ОПЕРАЦІЙНИХ СИСТЕМ

Один з етапів збору інформації про мережеві ресурси - визначення типу і версії ОС віддаленого вузла.

Всі відомі методи визначення ОС можна згрупувати наступним чином:

- найпростіші методи;
- TCP/IP Fingerprinting;
- засновані на використанні протоколу ICMP;
- маловідомі, рідко використовувані.

Розглянемо більш докладно наведені методи.

9.1. Найпростіші методи визначення ОС

До даної групи належать:

- аналіз наборів відкритих портів;
- використання сервісів прикладного рівня;
- аналіз банерів сервісів прикладного рівня;
- використання команд протоколів прикладного рівня;
- аналіз результатів ідентифікації сервісів і додатків.

Аналіз наборів відкритих портів. Найбільш простий метод заснований на очевидному факті, що ряд сервісів прикладного рівня жорстко «пов'язаний» з платформою. Наприклад, відкритий порт 22 (що часто використовується сервісом SSH) майже однозначно вказує на ОС UNIX, а порти 135, 139 - на ОС Windows (рис. 9.1).

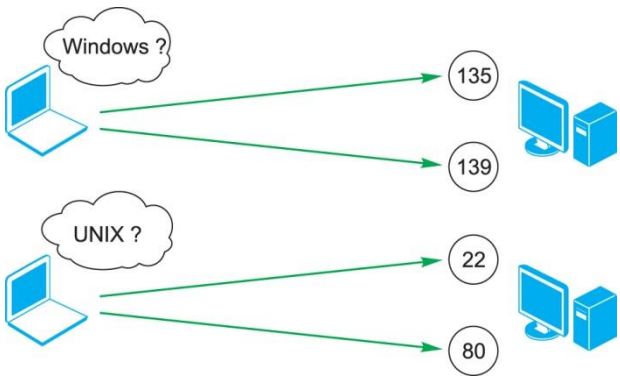


Рис. 9.1. Аналіз наборів відкритих портів

Використання сервісів прикладного рівня. Один з найпростіших методів визначення ОС віддаленого вузла - підключення на відкриті порти і аналіз відгуку працюючих на них служб (рис. 9.2).

9.2. Активна ідентифікація ОС — перспективи

На правильність результатів ідентифікації ОС сильно впливає взаємне

розташування скануючого і скануємого вузлів. Міжмережеві екрани ускладнюють визначення ОС скануємого вузла.

Для підвищення точності ідентифікації ОС має бути використано як можна більшу кількість різних тестів. Частина з них може закінчитися невдачею, якщо вжиті заходи щодо захисту скануємого вузла.

Досить часто складно розрізняти ОС, якщо вони відносяться до однієї групи (наприклад, Windows). У цьому випадку один із шляхів вирішення проблеми - ідентифікація служб об'єкту сканування вузла. Це побічно може допомогти при ідентифікації ОС.

Контрольні питання

1.Перерахуйте всі відомі методи ідентифікації операційних систем.

2.Перелічіть і дайте характеристику інструментарію для ідентифікації операційних систем.

Тема 10. ІДЕНТИФІКАЦІЯ ВРАЗЛИВОСТЕЙ ПО НЕ ПРЯМИХ ОЗНАКАХ

10.1. Методи ідентифікації вразливрстей по не прямих ознаках

Вище були розглянуті методи збору інформації про сканований об'єкт. В системах аналізу захищеності значна частина цієї інформації використовується для того, щоб зробити висновок про наявність уразливості. Такий спосіб називають ідентифікацією вразливостей за непрямими ознаками. В цілому перевірки, вбудовані в мережеві системи аналізу захищеності, можна класифікувати в такий спосіб (рис. 10.1).

Нижче розглянуті банерні і локальні перевірки.

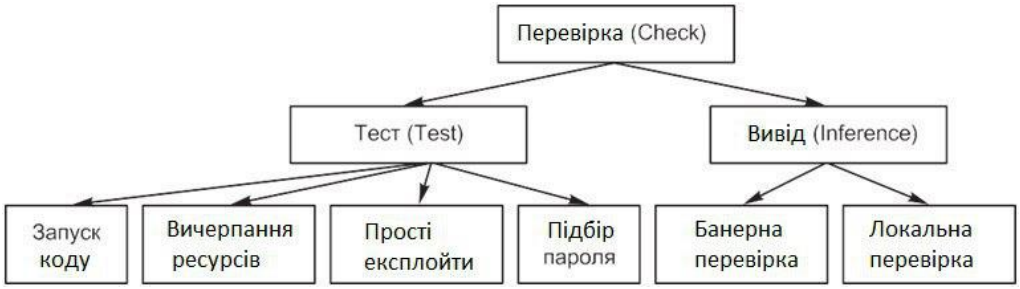


Рис. 10.1. Перевірки, вбудовані в мережеві системи аналізу захищеності

При цьому інформація може бути отримана через такі іменовані канали:

- \pipe\samr: SAM (Security Account Manager) RPC server;
- \pipe\lsarpc: LSA (Local Security Authority) RPC server;
- \pipe\netlogon: Netlogon RPC server;
- \pipe\svcctl: SCM (Service Control Manager) RPC server;
- \pipe\eventlog: Eventlog service RPC server;
- \pipe\srvsvc: Server service RPC server;
- \pipe\wkssvc: Workstation service RPC server.

Контрольні питання

1. Яким чином можна класифікувати перевірки, вбудовані в мережеві системи аналізу захищеності?
2. Якими способами виконуються перевірки щодо сервера DNS? Охарактеризуйте ці способи.
3. Як можна ідентифікувати вразливості на основі аналізу атрибутів файлу?
4. Яким способом можна зібрати інформацію про системи Windows?

Тема 11. PASSIVE FINGERPRINTING

Пасивна ідентифікація (PassiveFingerprinting) вузлів, ОС, служб і т. Д. Використовує ті ж методи аналізу інформації, що і активна, але реалізована інакше. Застосовуються різні способи отримання інформації, що підлягає аналізу. Пасивний метод використовує інформацію, «добровільно» розіслану досліджуваній системі. Він заснований (див. Вище) на наступних прийомах:

- аналіз меревого трафіку;
- аналіз запитів від сканованого вузла.

Таким чином, суть пасивної ідентифікації полягає в аналізі інформації, доступної без безпосереднього впливу на досліджувану систему. У сканерах безпеки ці методи або не реалізовані, або реалізовані не в повній мірі. Однак ці методи широко використовуються в сканерах безпеки для бездротових мереж.

11.1. Аналіз мережевого трафіку

Використання протоколу ARP. Утиліта arpscan (http://ish.cx/~jason/arpscan/) після запуску прослуховує трафік і аналізує прохідні по мережі arp-запити. На їх основі збирається інформація про використовувані IP-адреси в даному сегменті.

Протокол Telnet. При встановленні з'єднання по протоколу Telnet відбувається узгодження певних параметрів між серверною і клієнтською сторонами. Різні реалізації мають різні набори параметрів і їх порядок при узгодженні, що дозволяє ідентифікувати клієнтське ПЗ.

Електронна пошта (SMTP і POP3). Службові заголовки повідомлень електронної пошти містять детальну інформацію про відправника і процесі пересилання листа. У заголовках завжди є IP-адреса або ім'я вузла - відправника листа. Розгляд таких полів, як Message-ID, X-Mailer, User-Agent, дає можливість визначити клієнтське ПЗ, використане при написанні і відсиланні листа (аж до номера версії), і часто ОС клієнта, наприклад:

- Message-ID: (это Linux, Pine v4.10);
- X-Mailer: QUALCOMM Windows Eudora Version 4.3.2;
- X-Mailer: Microsoft Outlook Express 5.00.3018.1300.

Таким чином, механізм Passive Fingerprinting може бути використаний в наступних випадках:

• для збору інформації про мережу при проведенні аналізу захищеності внутрішньої мережі з використанням методології Penetrationtesting;

• виявлення невідомих пристроїв у мережі;

• інвентаризації ресурсів мережі (вузлів, ОС, служб) без впливу на продуктивність.

Контрольні питання

1. У чому полягає суть механізму PassiveFingerprinting?
2. Як відбувається аналіз мережевого трафіку з використанням пасивних методів?
3. Яким чином здійснюється пасивний збір інформації на основі аналізу даних різних віддалених клієнтів?
4.

Тема 12. ВИЯВЛЕННЯ ВРАЗЛИВОСТЕЙ ЗА ДОПОМОГОЮ ТЕСТІВ

Найбільш зрозумілий і очевидний спосіб пошуку будь-якої вразливості - спробувати використовувати її, т. Е. Імітація атаки, що її використовує. Відповідно до наведеного вище визначення, цей спосіб називається тестуванням. Застосування даного способу має певні складності, зокрема при оцінці:

• результатів тестування;

• вплив тестування на досліджувану систему.

12.1. Відмова в обслуговуванні

Окремого розгляду потребує завдання тестування вузлів на стійкість до «відмови в обслуговуванні». У загальному випадку задача зводиться до того, щоб після проведення тестування спробувати підключитися на потрібний порт і переконатися в тому, що підключення неможливо. Після цього робиться висновок про наявність уразливості. При цьому виникає ряд труднощів, наприклад вплив міжмережевих екранів і систем виявлення атак. Досить часто системи виявлення атак налаштовуються таким чином, що при виявленні DoS-атаки проводиться реконфігурація брандмауера, так що наступні підключення з боку скануючого вузла стають неможливі. В цьому випадку визначити причину недоступності системи складно. Ця проблема впливає на тести, перегляд результатів яких вимагає виконання окремої операції.

Деякі тести призводять до виведення з ладу всієї системи замість окремої служби. В цьому випадку виникає питання, якою є реальна причина виведення системи з ладу і чи пов'язана вона з тестуванням.

Контрольні питання

1. Які особливості виявлення вразливостей за допомогою тестів?
2. Що таке exploit check?
3. Як проводиться оцінка стійкості паролів?
4. В чому відмінність тестування від запуску «справжнього» эксплойта?
5. В чому полягає особливість тестування вузлів на стійкість до «відмови в обслуговуванні»?

Тема 13. МЕРЕЖЕВИЙ СКАНЕР NESSUS

Вище були наведені основні принципи аналізу захищеності, методи тестування різних служб, приклади інструментів для проведення тестів. Сканери безпеки, що розглядаються далі, поєднують в собі можливості окремих інструментів і реалізують різні методи сканування.

13.1. Огляд можливостей сканера

Nessus — сканер вразливостей, який може бути використаний для сканування одного або декількох вузлів мережі. Це вільно поширюваний інструмент сканування з регулярно оновлюваною базою перевірок. Розглянемо його основні характеристики і можливості.

Модульна архітектура. Кожна перевірка, що виконується сканером, являє собою зовнішній модуль (plugin). Це дозволяє легко додавати

Контрольні питання

1. Які можливості сканера Nessus?
2. Опишіть архітектуру сканера Nessus.
3. Який порядок отримання і установки сканера Nessus?
4. Опишіть порядок роботи сканера Nessus.

Тема 14. МОВА ОПИСУ АТАК NASL

Мова написання сценаріїв атак NASL (NessusAttackScriptingLanguage) розроблений спеціально для мережевого сканера Nessus. Він дозволяє швидко створювати сценарії (скрипти) з метою виявлення вразливостей вузлів мережі. Для версії сканера 2.0 мову NASL був повністю переписаний і отримав назву NASL2. Тести для сканера Nessus можуть бути також написані і на мові C.

Відзначимо переваги використання мови NASL:

- оптимізація для сканера Nessus;
- схожість с мовою C;
- безпека;
- простота модификації;

• переносимість.

До недоліків мови NASL можна віднести відсутність підтримки структур і засоби налагодження (існує виділений інтерпретатор NASL).

14.1. Структура сценарію

Загальні відомості. Після установки сценарії знаходяться в каталозі / usr / local / lib / nessus / plugins. Файли сценаріїв мають розширення .nasl, наприклад, account_lp.nasl. Структура вимагає наявності двох секцій: реєстрації (registersection) і опису атаки (attacksection).

Приклад заготовки для сценарію:

```
#
# Сценарій Nasl
#

if(description)
{ # #
# Секція реєстрації
# #

exit(0);
}

{
display("The remote FTP server seems to be tcp- wrapped\n");
}
close(soc);
}
```

Підключувані бібліотеки. Містять додаткові функції і реалізовані у вигляді файлів з розширенням .inc. Це в основному специфічні функції для роботи зі службами прикладного рівня.

Контрольні питання

1. Опишіть призначення і можливості мови NASL.
2. Перерахуйте функції NASL, які враховують особливості тестованих служб.

Тема 15. СКАНЕРИ БЕЗПЕКИ КОМПАНІЇ POSITIVE TECHNOLOGIES

На сучасному ринку засобів аналізу захищеності спостерігається переважання програмних комплексів, які позиціонують як системи управління вразливостями, які зазвичай включають в себе компоненти управління та скануючі модулі. Крім власне виявлення вразливостей такі програмні продукти мають можливості масштабування, формування звітів, інтеграції з іншими системами, адаптації під конкретну інформаційну систему, управління

інформаційними активами.

Фактично можна вважати, що сканер безпеки в такій системі представлений як окремий скануючий модуль. Таким чином, в даний час сканер безпеки може бути реалізований як окремий автономний програмний продукт або у вигляді модуля сканування в складі системи управління уразливими.

15.1. Коротка історична довідка

XSpider — сканер мережевого рівня (network-based), що виконує дистанційні перевірки вузлів мережі і не має розподіленої архітектури (рис. 15.1).

Сканер безпеки XSpider з'явився 2 грудня 1998 р Перша версія цього сканера називалася Spider, але незабаром сканер був перейменований в XSpider. У 2000 р програма XSpider була викладена в мережі Інтернет для вільного скачування.

Комерційна версія сканера XSpider 7.0 з'явилася в 2002 р, в цьому ж році була створена компанія PositiveTechnologies. Спочатку основним напрямком діяльності компанії були послуги в області захисту інформації: аудит зовнішніх і внутрішніх мереж і ін. (Internet Information Server, Apache і т. Д.), А також встановлених розширень (FrontPage, OpenSSL і т. П.).

Наступним етапом є авторизація та перевірка добре відомих вразливостей web-додатків.

Після цього включається механізм пошуку прихованих директорій і індексації вмісту. В ході збору вмісту скануючий ядро XSpider використовує не тільки вміст web-сторінок. Різні службові та інформаційні файли, що містяться на сервері (наприклад, robots або readme.txt), також аналізуються на предмет наявності гіперпосилань. У XSpider входить базовий аналізатор JavaScript, що дозволяє працювати з AJAX-додатками.

Після побудови карти сайту сканер переходить до режиму пошуку вразливостей, які відображаються в консолі програми по мірі виявлення.

Контрольні питання

1. Опишіть архітектуру і основні можливості сканера XSpider.
2. Перерахуйте етапи роботи сканера XSpider.
3. Яким чином здійснюється ідентифікація вразливостей?
4. Як проводяться локальні провірки систем Windows?
5. Яким образом відбувається виявлення вразливостей web-додатків?

Тема 16. АНАЛІЗ ЗАХИЩЕНОСТІ НА РІВНІ ВУЗЛА

Раніше були розглянуті сканери мережевого рівня, що виконують дистанційні перевірки. Мережевий сканер ідентифікує уразливості найвищого ступеня ризику, які вимагають негайного реагування. Дана Тема присвячена сканерам рівня вузла (host-based). Такі сканери, встановлені безпосередньо на сканований вузол, виконують перевірки локально. Розглянемо їх особливості, принципи роботи, які вирішуються завдання, а також оцінку стійкості паролів.

16.1. Задачі локального сканування

Сканери рівня вузла здійснюють пошук вразливостей ретельніше і вірогідно, оскільки встановлені на сканованому вузлі і працюють від імені облікового запису з максимальними привілеями (root, SYSTEM). Сканери виконують ті ж перевірки, що і мережеві сканери. Наприклад, вони можуть здійснювати пошук працюють на вузлі пристроїв, таких як модеми, а також виявляти встановлені на вузлі додатки або контролювати режим роботи мережевого адаптера (селективний або неселективний). За допомогою сканерів рівня вузла доцільно виконувати ті перевірки, які неможливі або важко виконати для мережевих сканерів або займають багато времені.Результати зберігаються локально, а потім передаються на консоль.

В контексті AssuriaAuditor сесія сканування визначається безліччю агентів, до яких застосовується будь-яка політика сканування. Сканування з цією політикою запускається одночасно на всіх агентів, що входять у цю множину.

Політика сканування - це набір груп перевірок, що виконуються одночасно.

У сканера AssuriaAuditor є особливість, згідно з якою перевірки об'єднуються в групи (по типу), а потім групи об'єднуються в політику сканування.

Контрольні питання

1. Перелічіть завдання локального сканування. Дайте характеристику кожного завдання.
2. Які особливості архітектури сканерів рівня вузла?
3. Яким чином здійснюється ідентифікація вразливостей?
4. Перерахуйте джерела даних для сканерів рівня вузла.
5. Що таке сканер AssuriaAuditor?

Тема 17. СПЕЦІАЛІЗОВАНІ ЗАСОБИ АНАЛІЗУ ЗАХИЩЕНОСТІ

17.1. Клаифікація сканерів безпеки за призначенням

Застосовується також класифікація сканерів безпеки за їх призначенням. При цьому виділяють дві категорії: сканери загального характеру і спеціалізовані сканери.

Пояснити цей спосіб класифікації на прикладі мережевих сканерів можна наступним чином. Перевірки, виконувані мережевими сканерами безпеки, спрямовані насамперед на мережеві служби. Звичайно, при цьому здійснюється пошук вразливостей не тільки мережевих служб, а й ОС, а також деяких додатків, встановлених на сканованому вузлі. Але слід визнати, що перевірки, вбудовані в мережеві сканери, носять загальний характер, а якщо і спрямовані на програми, то це найбільш поширені програми та найбільш відомі

уразливості. Та ж ситуація і з сканерами рівня вузла. Їх перевірки, можливо, трохи більше спрямовані на ОС вузла, де встановлений агент, а також можуть бути спрямовані і на конкретні програми, але жодне з них не виділяється. Таким чином працюють сканери загального характеру. Іншими словами, в них «всього потроху». Частина перевірок, наприклад, спрямована на пошук вразливостей

17.4. Приклади програм-сканерів вразливостей СУБД

Засоби аналізу захищеності СУБД дозволяють проводити і локальний, і дистанційний аналіз серверів БД. Як приклади можна навести такі системи:

• AppSentry компании Integrity(http://www.integrigy.com/products/appsentry);

• AppDetectivePro компании Trustwave (https://www.trustwave.com/ Products/Database-Security/);

• продукты компании NGSSecure (http://www.ngssecure.com/services/ information-security-software.aspx);

• McAfee Security Scanner for Databases (http://www.mcafee.com/us/ products/security-scanner-for-databases.aspx);

• Shadow Database Scanner компании Safety Lab (http://www.safety-lab. com/en/products/6.htm /);

• SecureSphere Discovery and Assessment Server (http://www.imperva. com/products/dsc_database-discovery-and-assessment-server.html);

• Scuba (http://www.imperva.com/products/dsc_database-discovery-and-assessment-server.html).

Контрольні питання

1. Як класифікувати сканери безпеки за призначенням?
2. Дайте характеристику загрозам і вразливостям СУБД.
3. В чому полягають особливості аналізу захищеності СУБД?
4. Наведіть приклади програм-сканерів вразливостей СУБД. Як їх використовувати?

Тема 18. МЕТОДОЛОГІЯ АНАЛІЗА ЗАХИЩЕНОСТІ ETHICAL HACKING

18.1. Необхідність методології аналізу захищеності

Вище були розглянуті можливості сканерів вразливостей і наголошено на необхідності методології при аналізі захищеності. Однак покладатися тільки на результати роботи сканера вразливостей не можна. На основі цих результатів можна зробити наступні дії:

• встановити оновлення відповідно до знайдених вразливостей;

• провести заходи щодо зниження ймовірності використання вразливості, якщо вона не може бути усунена негайно (наприклад, внаслідок проблем

сумісності);

• перевірити правильність (коректність) усунення вразливостей;

• внести зміни в політику безпеки, архітектуру системи з метою врахування останніх змін.

Обмеження методології PenetrationTesting. Результати тестування на стійкість до злому (PenetrationTesting) не слід розглядати як остаточний висновок про ступінь захищеності об'єкта тестування. Вже згадана методологія має наступні обмеження:

- тестований об'єкт (мережа, окремий вузол і т. П.) Розглядається як «чорний ящик». Отже, тестуючий спочатку володіє мінімумом інформації про об'єкт тестування, тому багато уразливості можуть бути не виявлені. Для їх виявлення необхідно мати певну інформацію про тестуючу систему (якою, наприклад, може мати внутрішній користувач);
- тестування відбувається в якийсь обмежений період часу, отже, результати визначаються відомими в даний момент вразливостями і поточною конфігурацією мережі. Ситуація може змінитися на наступний же день. Перевірка мережі на стійкість до злому внаслідок її високої вартості і можливого негативного впливу на об'єкт тестування проводиться нечасто (наприклад, один раз на рік).

Таким чином, до результатів тестування з використанням розглянутої методології слід поставитися серйозно. Якнайшвидше дані повинні бути надані керівництву. На основі результатів тестування можуть бути зроблені наступні дії:

- усунення виявлених і підтверджених вразливостей;
- перегляд політики безпеки і внесення змін;
- • підвищення кваліфікації персоналу та інші заходи, спрямовані на підвищення захищеності систем.

Слід розуміти, що основне обмеження даної методології полягає в тому, що проводиться ідентифікація не всіх вразливостей. Це лише погляд на об'єкт тестування з точки зору «реального» порушника, якому, наприклад, для отримання доступу до вузла досить виявити одну-дві серйозні вразливості.

Тому необхідно проводити оцінку захищеності мережі силами самої організації і з більшою періодичністю. Але це вже інша методологія: Vulnerability assessment або Network Security Assessment. Фактично це передбачає впровадження аналізу захищеності в корпоративній мережі як частини політики безпеки, що розглядається в гл. 19.

Контрольні питання

1. Обгрунтуйте необхідність методології аналізу захищеності.
2. Що входить в поняття «PenetrationTesting»?
3. Перечисліть особливості PenetrationTesting зсередини і зовні.

4. Перечислить этапи PenetrationTesting. Дайте характеристику кожному етапу.

5. По яких причинах застосування методології PenetrationTesting може бути обмежено?

Тема 19. ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ВРАЗЛИВОСТЯМИ

19.1. Необхідність централізованого управління вразливостями

Сканери безпеки як один з видів ПО відомі більш 10 років. Але до сих пір їх застосування в якості засобів забезпечення безпеки викликає безліч дискусій. І не тільки тому, що мережевий сканер безпеки - це продукт «подвійного» призначення і можливі негативні наслідки його використання, а через механізм захисту, який в ньому реалізований.

Сам по собі сканер безпеки як інструмент, що дозволяє на виході отримати перелік вразливостей перевіреної їм системи, потрібен не всім. Він може, наприклад, допомогти фахівця при проведенні тестування на проникнення автоматизувати частину рутинної роботи або виявитися корисним для зловмисника, який шукає слабкості в системі для отримання до неї несанкціонованого доступу. Для ефективного застосування сканерів безпеки в корпоративній мережі необхідна їх інтеграція в існуючу інфраструктуру забезпечення безпеки. Тому на зміну сканерів безпеки в корпоративному секторі поступово приходять системи управління уразливими. Сканер безпеки в такій системі - всього лише один з модулів, що надає інформацію для інших модулів або компонентів, а також для інших систем.

Управління вразливостями - це процес, а не готовий продукт, але цей процес можна автоматизувати. Власне, для цього і потрібні системи управління уразливими.

У найзагальнішому розумінні, управління вразливостями (VulnerabilityManagement) - процес, спрямований на запобігання використання відомих вразливостей, потенційно існуючих в системі, що захищається або мережі. Основний очікуваний результат - значне усладнення або повне виключення можливостей для порушників використання цих вразливостей і, відповідно, зниження витрат на ліквідацію наслідків атак.

Створити абсолютно захищену систему принципово неможливо. До того ж нові вразливості в комп'ютерних системах, у використовуваному ПО виявляються досить регулярно. Згідно зі статистичними даними, які легко можна отримати на основі відомого каталогу вразливостей (http://web.nvd.nist.gov), число вразливостей, які виявляються щорічно, становить 5 ... 6 тис. І більше.

І це тільки вразливості реалізації, а є ще помилки проектування і експлуатації. Адже в процесі експлуатації система може змінюватися.

Зрозуміло, розмір потенційних збитків від використання конкретної уразливості в конкретній системі, що захищається може бути досить різні.

19.4. Усунення вразливостей і контроль

Усунення вразливостей. Це найбільш складний і трудомісткий етап. Складність полягає в тому, що саме на цьому етапі доводиться вносити зміни в корпоративну інформаційну систему. Отже, по кожній уразливості або відхиленню з отриманого на попередньому етапі списку потрібно приймати рішення (усунути, залишити як є, розібратися і т. д.).

Після прийняття рішення про усунення вразливості слід обґрунтований вибір варіанта усунення, в разі необхідності можна вдатися до тестування, оскільки внесення в систему змін може привести до її непрацездатності.

На практиці зазвичай доводиться вибирати один із наступних варіантів:

- оновлення системи;
- встановлення «патча»;
- перехід на нову версію;
- зміна конфігурації (workaround);
- відмова від використання вразливого ПО.

Після вибору варіанту усунення проводиться власне усунення вразливості, яке може відбуватися автоматично (в окремих випадках) або вручну. В останньому випадку може знадобитися розробка рекомендацій для осіб, задіяних в цьому процесі. Звичайною практикою при цьому є процес формування заявок для систем типу HelpDesk, ServiceDesk або інших систем управління заявками. Відповідний функціонал може входити і в саму систему управління вразливостями.

Таким чином, на цьому етапі система повинна забезпечити відповідний workflow, починаючи від прийняття рішення про вразливості і закінчуючи формуванням заявки і призначенням відповідального.

Контроль. Остання складова процесу управління вразливостями - контроль правильності усунення вразливостей. Контроль може бути виконаний різними способами, наприклад:

- шляхом використання скануючих модулів;
- аналізу журналів відповідних систем.

При цьому можуть бути ефективні порівняльні звіти, функціонал відстеження змін або навіть можливість відстеження динаміки зміни стану захищеності системи.

Контрольні питання

1. Чим викликана необхідність централізованого управління вразливостями?
2. Розкрийте суть інвентаризації інформаційних активів.
3. Перелічіть завдання і способи моніторингу стану захищеності.
4. До чого зводиться усунення вразливостей?
5. Якими способами здійснюється контроль правильності усунення

вразливостей?

Тема 20. КОНТРОЛЬ ЗАХИЩЕНОСТІ БЕЗДРОТОВИХ МЕРЕЖ

20.1 Особливості сканування бездротових мереж

У попередніх розділах було розглянуто два завдання, які вирішуються сканерами: збір інформації та ідентифікація вразливостей. Збір інформації про систему може виконуватися двома способами:
1) ActiveFingerprinting - використання ключових впливів на систему і аналіз відгуків;
2) PassiveFingerprinting - використання інформації, «добровільно» розсилається досліджуваної системою.

Якщо для сканування звичайної мережі зазвичай використовуються активні методи збору інформації, то для бездротової мережі частина перевірок грунтується на пасивному аналізі трафіку. Таким чином, головна особливість сканування бездротових мереж полягає в поєднанні активних методів збору інформації та пасивного прослуховування ефіру. При цьому пасивні методи явно переважають. Тому сканери для бездротових мереж не набули широкого поширення.

20.2 Сканери для бездротових мереж

Завдання сканування бездротових мереж. На мережевому рівні і вище аналіз захищеності бездротових мереж принципово не відрізняється від аналізу захищеності вузлів звичайної мережі. Слід зазначити лише процедуру сканування точки доступу як об'єкта, що має IP-адресу і відкриті порти.

Уразливості, характерні для бездротових мереж. Як зазначалося вище, аналіз захищеності бездротової мережі складається з двох частин:

1) явне підключення до точки доступу та виконання перевірок;

2) прослуховування трафіку і виявлення різних проблем. До першої частини можна віднести наступні перевірки:
• можливість підключення до точки доступу (без аутентифікації, не повідомляючи ключа і т. П.);
• можливість отримання IP-адреси у сервера DHCP, вбудованого в точку доступу;
• можливість конфігурування точки доступу через бездротовий інтерфейс.
Останню перевірку слід розглянути більш детально. Оскільки точка доступу має IP-адресу (для її конфігурації), він однаково використовується як з проводовим інтерфейсом, так і з бездротовим. Це означає,що існує загроза підключення до точки доступу через бездротовий інтерфейс для зміни налаштувань. Однак ця адреса використовується виключно для конфігурації точки доступу і не впливаєна роботу.
Приклади кроків, виконуваних на данному етапі:
• видалення призначених для користувача обліковихзаписів, створених в процесс і тестування;
• відновлення систем, до яких був отриманий доступ;

• відновлення систем, виведених з ладу.
Цей етап може виконуватися і силами організації, яка замовила проведення тестування. Слід зазначити, що в будь-якому випадку повинен бути наданий детальний перелік внесених в процесс і тестування змін.

Контрольні питання

1. У чому полягають особливості сканування бездротових мереж?
2. Перелічіть авдання сканування бездротових мереж.
3. Які уразливості, характерні для бездротових мереж?
4. Опишіть методологію сканування точки доступу на мережевому рівні.
5. У чому полягає методологія аудиту бездротових мереж?

Тема 21. ДЖЕРЕЛА ДАНИХ ДЛЯ СИСТЕМ ВИЯВЛЕННЯ АТАК

21.1. Складовітехнологіївиявлення атак

У загальному випадку система виявлення атак складається з компонентів двох типів: компоненти управління та агенти (сенсори, модулі стеження). При цьому зазвичай до складу компонентів управління входять клієнтські (керуюча консоль) і серверні компоненти різного призначення (рис. 21.1). Наприклад, до складу рішення по виявленню атак IBM Security входять сенсори для захисту сегментів і окремих вузлів, як системи управління використовується система SiteProtector, підключитися до неї користувачі можуть або за допомогою консолі, або через web-інтерфейс (рис. 21.2).

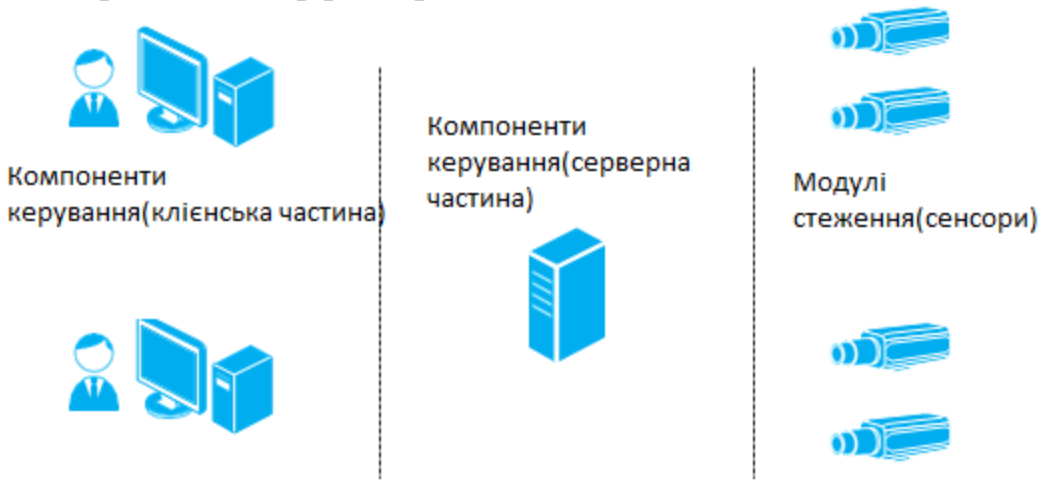


Рис. 21.1. Компоненти системи виявлення атак

Потік (Flow) - «однонаправлена» послідовність мережевих пакетів між двома вузлами мережі. Однозначно визначається наступними атрибутами:

• sourceIPaddress;
• destinationIPaddress;
• source port number;
• destination port number;
• protocol type;
• type of services;
• routerinputinterface.

Дані про потоці можуть включати в себе:

• кількість переданих даних;

• час початку (закінчення) з'єднання. Архітектура Network Flow приведена на рис. 21.29.

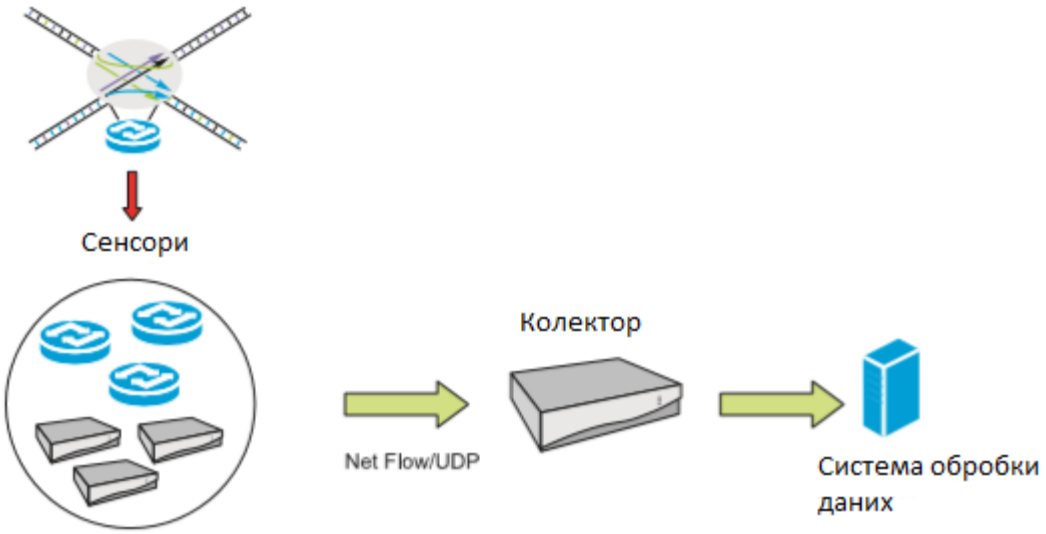


Рис. 21.29. Архітектура NetworkFlow

Перший стандарт в цій області - протокол sFlow (RFC3176) - призначений для моніторингу трафіку в комутованих і сегментованих мережах. В даний час на статус стандарту претендує протокол IPFIX (IPFlowInformationeXport).

Контрольні питання

1. Перелічіть складові технології виявлення атак.
2. Опишіть архітектуру мережевої IDS, її переваги і недоліки.
3. У чому полягає специфіка виявлення атак на рівні вузла? Опишіть її переваги і недоліки.
4. Як використовувати особливості архітектури NetworkFlow для виявлення атак?

Тема 22. ОЗНАКИ АТАК

При виявленні атаки практично завжди можна назвати характерні ознаки, на основі яких було зроблено висновок про наявність атаки. Наприклад, події, наведені в фрагменті журналу системи виявлення атак snort на рис. 22.1, були зафіксовані внаслідок використання при підключенні до сервера FTP «характерних» імен (в команді USER).

```
[**] [1:144:10] FTP ADMw0rm ftp login attempt [**]
[Classification: An attempted login using a suspicious username was
riority: 2]
12/18/08-12:44:45.557224 192.168.108.224:34398 -> 192.168.104.252:21
TCP TTL:64 TOS:0x10 ID:20814 IpLen:20 DgmLen:63 DF
***AP*** Seq: 0x110354AF  Ack: 0xA8EC2314  Win: 0xB7  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4008388 248409
[Xref => http://www.whitehats.com/info/IDS01]

[**] [1:354:6] FTP iss scan [**]
[Classification: An attempted login using a suspicious username was
riority: 2]
12/18/08-12:44:56.969168 192.168.108.224:34398 -> 192.168.104.252:21
TCP TTL:64 TOS:0x10 ID:20816 IpLen:20 DgmLen:67 DF
***AP*** Seq: 0x110354BA  Ack: 0xA8EC2335  Win: 0xB7  TcpLen: 32
TCP Options (3) => NOP NOP TS: 4019800 248501
[Xref => http://www.whitehats.com/info/IDS331]
```

Рис. 22.1. Фрагмент журналу системи виявлення атак snort

Ознаки, на основі яких можна зробити висновок про наявність атаки, можуть бути найрізноманітнішими. Крім того, вони можуть залежати від конкретного оточення, наприклад, в одному випадку ознакою атаки є передача по мережі файлу з певним вмістом, в іншому - підключення до сервера з певного адреси.

Розуміння ознак атак важливо при аналізі подій, так як дозволяє точно вказати причину спрацювання тій чи іншій сигнатури.

Запропонувати повний перелік ознак атак досить проблематично, вкажемо деякі з них:

- використання вразливостей;
- відхилення від граничних значень;
- використання відомих технік та інструментів для проведення атак;
- відхилення від відомих моделей поведінки мережевих протоколів.

22.1. Використання вразливостей як ознака атаки

Зазвичай для атаки використовується будь-яка вразливість. Тому практично будь-якій атаці можна поставити у відповідність використовувану при її проведенні вразливість. У зв'язку з цим багато ознак атак будуються на

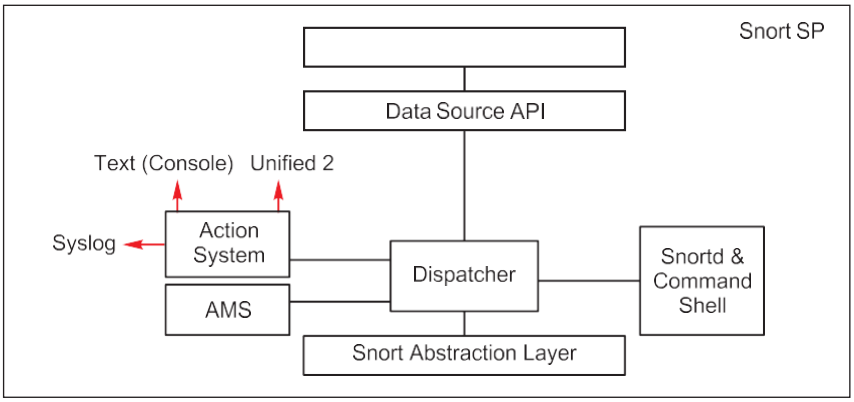


Рис. 22.16. Варіанти реагування

За замовчуванням snortsp при запуску шукає файл з такою назвою в каталогах / etc, / etc / snort або / usr / local / snortsp / etc (в зазначеному порядку). Зразок файлу snort.lua можна знайти в каталозі …/snortsp-3.0.0b2/etc

Таким чином, можна або підготувати файл, звідки snortsp буде брати необхідну інформацію при запуску, або після запуску «побудувати» потрібну конфігурацію вручну.

Загальний порядок роботи в середовищі SnortSP наступний:

1) конфігурація модулів source, engine, analyzer, output. В результаті конфігурації виходить набір об'єктів;

2) «зв'язування »створених об'єктів між собою;

3) запуск модуля engine;

4) після запуску можна управляти модулем engine, користуючись інтерфейсом командного рядка.

Контрольні питання

1. Опишіть використання вразливостей як ознака атаки.

2. У чому полягає ознака атаки «відхилення від граничних значень»? Наведіть приклади.

3. Опишіть використання відомих технік та інструментів для проведення атак.

4. Розкажіть про систему виявлення атак Snort. КакіеIDS використовуються на практиці? Які їх переваги та недоліки?

Тема 23. МЕТОДИ ВИЯВЛЕННЯ АТАК

Існують два методи виявлення атак:

• на основі знання всіх можливих атак і їх модифікацій;

• на основі розуміння очікуваної поведінки контрольованого об'єкта.

23.1. Виявлення «зловживань»

Перший метод називається виявленням «зловживань», джерелами даних в ньому служать журнали, мережевий трафік.

Сигнатура (signature) — сукупність параметрів, «відбиток» (pattern), відповідний відомій атаці.

Виявлення «зловживань» — процес зіставлення сигнатур і пройшли попередню обробку даних (отриманих з відповідних джерел) для ідентифікації можливих інцидентів.

Приклади сигнатур:

• спроба отримання по протоколу ftp файла /etc/passwd;

• поява в журналі аудиту події з ідентифікатором 645;

• спроба підключення до закритого в даний момент TCP-порту.

В якості найпростішого прикладу можна навести мережеву систему

виявлення атак, що займається синтаксичним аналізом окремих пакетів. Метод синтаксичного аналізу застосовувався в перших мережевих IDS.

Пізніше він був удосконалений шляхом додавання нових можливостей (рис. 23.1),

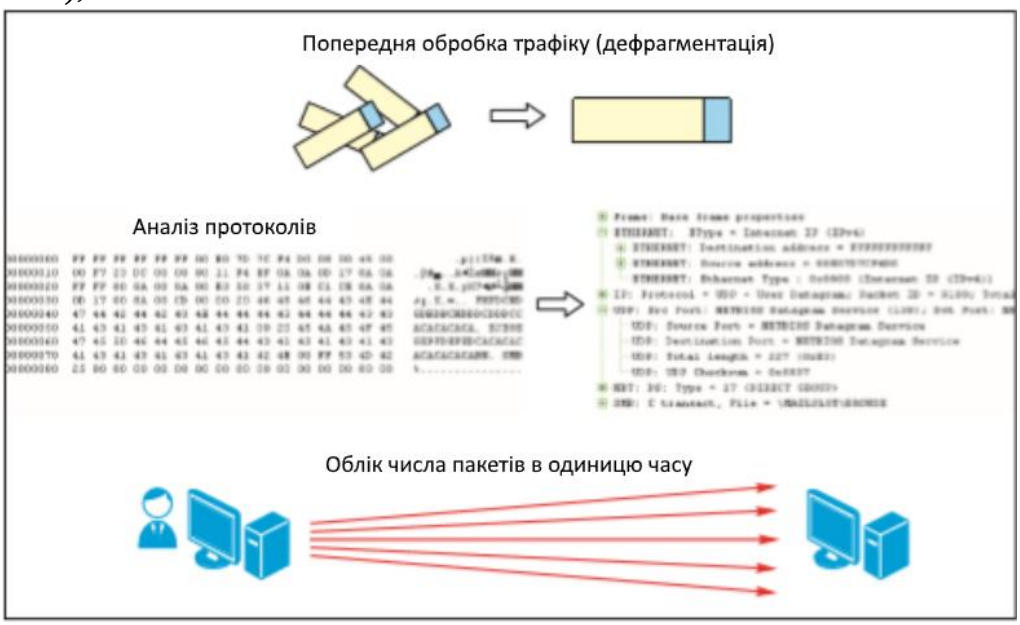


Рис. 23.1. Додаткові можливості до синтаксичному аналізу окремих пакетів

- відношення між вузлами і групами вузлів;
- архів потоків даних.

Приклад моделі відносин між вузлами мережі наведено на рис. 23.7.

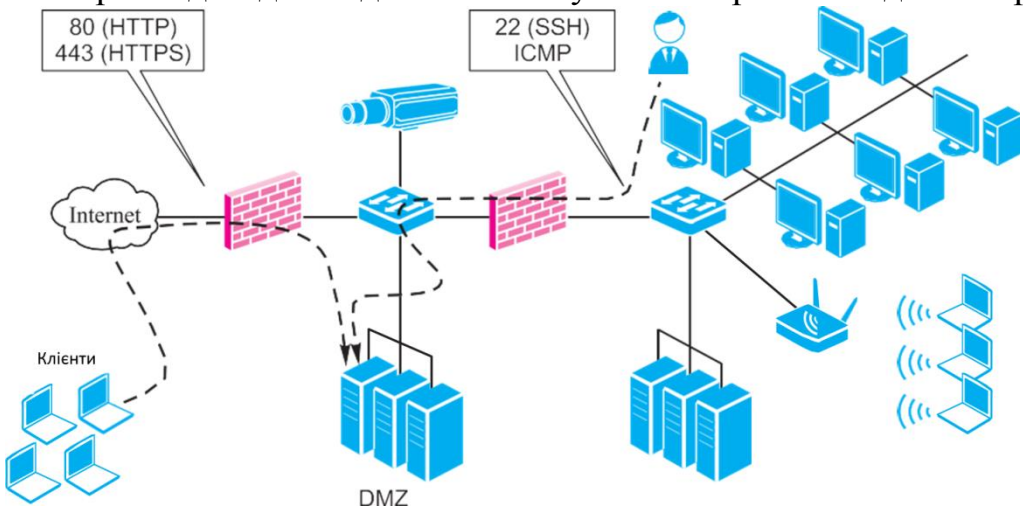


Рис. 23.7. Модель відношення між вузлами мережі

Метод виявлення аномалій може бути використаний як доповнення до методу виявлення «зловживань» для виявлення:

- відхилень в трафіку за часом і обсягом;
- нетипових підключень;
- недоступних вузлів і сервісів.

Контрольні питання

1. Опишіть переваги та недоліки методу виявлення «зловживань».
2. У чому полягає алгоритм виявлення атак методу виявлення аномалій? Назвіть його переваги і недоліки.

Тема 24. МЕХАНІЗМИ РЕАГУВАННЯ

24.1. Огляд механізмів реагування

Як зазначалося вище, механізми реагування відрізняються різноманітністю. Проте їх можна використовувати в якості критерію для поділу систем на два типи: виявлення атак і протидії атакам.

На рис. 24.1 представлені різні варіанти оповіщення. Варіанти реєстрації подій представлені на рис. 24.2.

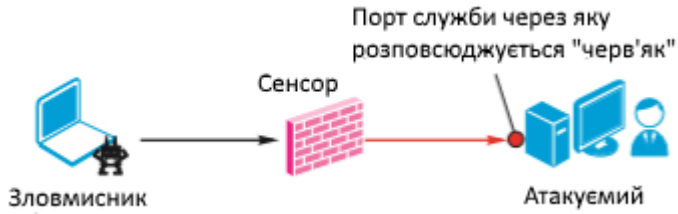


Рис. 24.8. Карантин і ізоляція «черв'яка»

Видно, що механізм блокування «перетворює» систему виявлення атак в систему протидії атакам. Це накладає додаткові вимоги, зокрема:

- наявність сценарію дій для NetworkIPS в разі виходу його з ладу;
- наявність «м'якого» режиму;
- відсутність впливу на продуктивність;
- якість сигнатур, мінімізація помилкових спрацьовувань.

Для блокування порушника можуть бути застосовані і стандартні рішення щодо забезпечення відмовостійкості, з використанням вбудованого або зовнішнього модуля Bypass (рис. 24.9).

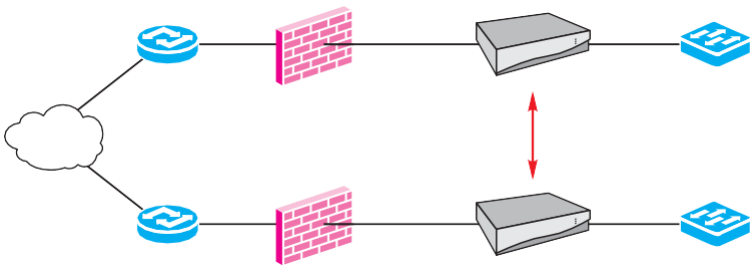


Рис. 24.9. Стандартні рішення щодо забезпечення відмовостійкості

Наявність «м'якого» режиму означає можливість щодо простого і швидкого вимикання механізму блокування і (або) заміни його записом в журнал.

Контрольні питання

1. Які механізми реагування можуть бути реалізовані в системах виявлення атак?
2. Якими способами може бути виконано блокування порушника?

Тема 25. ВИЯВЛЕННЯ АТАК В БЕЗДРОТОВИХ МЕРЕЖАХ

25.1. Загрози, пов'язані з використанням бездротових мереж

На рівні IP для бездротових мереж характерні ті ж проблеми безпеки, що і для звичайних мереж. Але на канальному і фізичному рівнях особливість бездротових мереж - передача даних «по повітрю» і відсутність кабелів для підключення до мережі - вносять деяку специфіку. Відносна легкість підключення означає, що доступ до мережі може бути отриманий, наприклад, із сусідньої кімнати, коридору та, можливо, з вулиці.

У зв'язку з цим виникає перша загроза, що представляє собою несанкціоноване підключення до ресурсів бездротової мережі і використання її ресурсів (рис. 25.1).

Друга загроза - можливість пасивного прослуховування переданих в ефірі даних (рис. 25.2). Для цього досить перевести бездротової адаптер в неселективний режим (для бездротових мереж цей режим називають режимом моніторингу), налаштувати на потрібний канал і здійснювати перехоплення трафіку бездротових мереж, що знаходяться в радіусі дії антени.

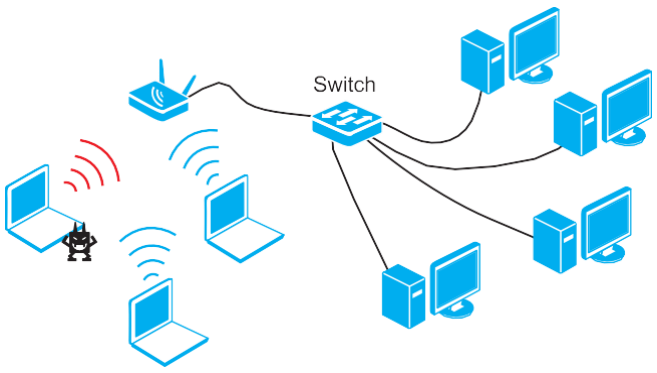


Рис. 25.1. Несанкціоноване підключення

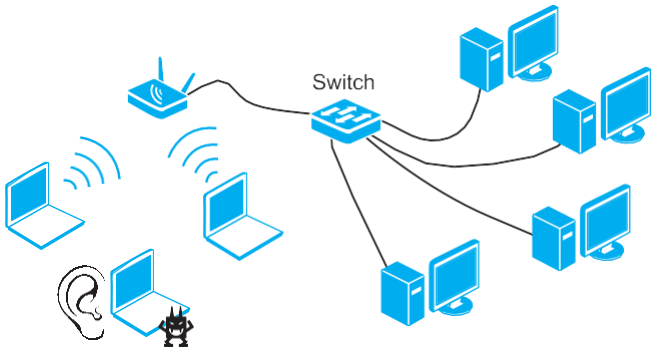


Рис. 25.2. Прослуховування трафіку беспровідної мережі

WLAN можуть діяти різні політики безпеки (основна мережа, гостьова мережа).

Система AirMagnet може використовувати такі конфігуруються критерії для визначення приналежності точки доступу і клієнта мережі компанії:

- використовуваний канал 802.11b/g/a;
- ідентифікатор виробника в MAC-адресі (IEEEOUI);
- реалізації протоколу 802.11 (802.11a, 802.11b, 802.11g або різні поєднання);
- адреса канального рівня MAC-адрес;
- ідентифікатор мережі (SSID).

Для кожної з категорії можна задати «білі списки» MAC-адрес, ідентифікаторів OUI і т. д., виявлення яких не викликає спрацьовування сигнатури.

При цьому контролюється використання наступних технологій захисту бездротових мереж:

- шифрування (любое);
- аутентификация Open System/Shared Key;
- віртуальні приватні мережі на основі L2TP, IPSec, PPTP, SSH;
- технологія 802.1x (динамічні ключі WEP);
- шифрування TKIP (WPA);
- аутентифікація Protected EAP (PEAP);
- шифрування на загальних ключах (WPA-PSK, 802.11i-PSK);
- аутентификация EAP-FAST;
- шифрування AES (802.11i);
- шифрування Fortress;
- шифрування Cranite.

Контрольні питання

1. Перерахуйте загрози безпеки по відношенню до бездротових мереж.
2. У чому полягає несанкціоноване використання бездротових пристроїв?
3. Які завдання вирішуються в ході моніторингу безпеки бездротової мережі?
4. Які особливості виявлення атак в бездротових мережах?
5. Сформулюйте перелік атак, специфічних для бездротових мереж.
6. Наведіть приклади систем виявлення атак в бездротових мережах.

Тема 26. ІНТЕГРАЦІЯ ЗАСОБІВ ВИЯВЛЕННЯ ТА ЗАПОБІГАННЯ АТАК В ЄДИНУ СИСТЕМУ І ВЗАЄМОДІЯ З ІНШИМИ ЗАСОБАМИ ЗАХИСТУ

У багатьох випадках рішення по виявленню і запобіганню атак будується з використанням різних (розглянутих вище) технологій. Поряд з мережевими системами виявлення атак можуть застосовуватися системи захисту серверів і робочих станцій, а також спеціалізовані системи захисту від атак.

На додаток до цього одна і та ж технологія може бути реалізована в різних продуктах (наприклад, від різних виробників). Спільне застосування таких продуктів може бути обумовлено бажанням підвищити відмовостійкість системи в цілому або зменшити число помилкових спрацьовувань.

Нарешті, поряд з системами виявлення і запобігання атак в корпоративній мережі застосовуються і інші засоби захисту. Часто взаємодіє ствие цих засобів між собою підвищує ефективність захисту в цілому.

26.1. Інтеграція засобів виявлення і запобігання атак в єдину систему

З метою захисту досить часто використовуються продукти і технології від одного вендора, наприклад, спільне застосування засобів виявлення атак рівня мережі (network-based) і рівня вузла (host-based). В цьому випадку їх інтеграція в єдину систему - це централізоване управління засобами виявлення різних атак за допомогою єдиної консолі (рис. 26.1).

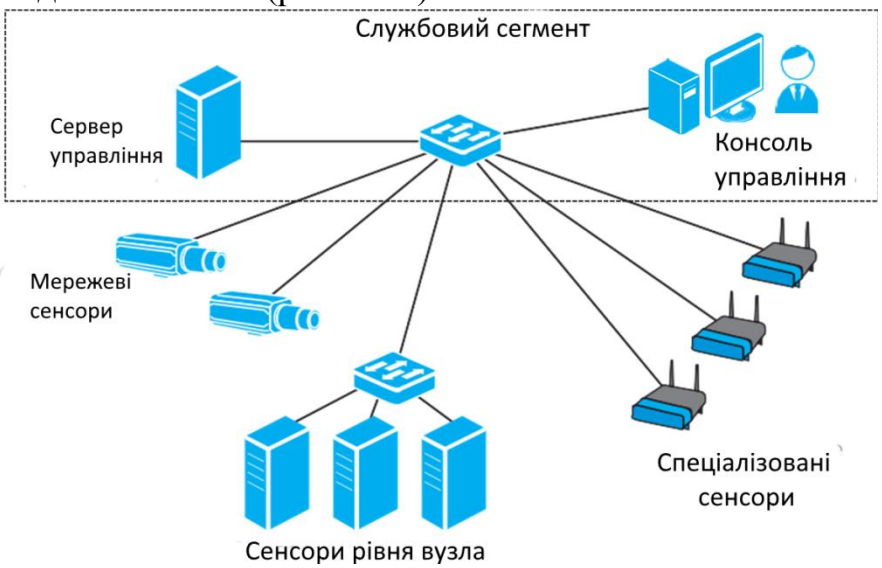


Рис. 26.1. Спільне застосування засобів виявлення атак рівня мережі і рівня вузла

В цілому потрібно зіставляти такі дані:

- інші події, виявлені тим же сенсором;
- журнали посередників (proxy), міжмережевих екранів;
- результати роботи сканерів безпеки;
- журнали антивірусних систем.

Контрольні питання

1. 1. Яким способом можна провести інтеграцію IDS / IPS в єдину систему?
2. Наведіть приклади кореляції даних, отриманих з різних джерел, для виявлення атак.

Література

1. Абрамов Е.С., Сидоров И.Д. Метод обнаружения распределенных информацион- ных воздействий на основе гибридной нейронной сети // Известия ЮФУ. Техниче- ские науки. 2009. № 11 (100). С. 154–164.
2. Аткина В.С. Применение иммунной сети для анализа катастрофоустойчивости информационных систем // Известия ЮФУ. Технические науки. 2011. № 12 (125). С. 203–210.
3. Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информа- ции: учеб. пособие. 3-е изд. М.: ИЦ РИОР; НИЦ ИНФРА-М, 2016. 322 с.
4. Будько М.Б., Будько М.Ю. Отслеживание изменений в структуре сети и решение задач повышения безопасности на основе анализа потоков данных // Научно-техни- ческий вестник Санкт-Петербургского государственного университета информаци- онных технологий, механики и оптики. 2009. № 59. С. 78–82.
5. Жук А.П., Жук Е.П., Лепешкин О.М., Тимошкин А.И. Защита информации: учеб.пособие. 2-е изд. М.: ИЦ РИОР; НИЦ ИНФРА-М, 2015. 392 с.
6. Ищейнов В.Я., Мецатунян М.В. Основные положения информационной безопас- ности: учеб. пособие. М.: ИД «Форум»; НИЦ ИНФРА-М, 2015. 208 с.
7. Максимова Е.А., Корнева В.А. Оптимизация технологии безопасного информа- ционного взаимодействия в корпоративных системах // Матер. XII Междунар. на- уч.-практ. конф. «ИБ-2012». Ч. II. Таганрог: Изд-во ТТИ ЮФУ, 2012. С. 124–129.
8. Максимова Е.А., Корнева В.А. Формализация действий злоумышленника при прогнозировании вторжений в корпоративную информационную систему // Акту- альные вопросы информационной безопасности регионов в условиях глобализации информационного пространства. Матер. II Всеросс. науч.-практ. конф., Волгоград, 26 апреля 2013 г. Волгоград: Изд-во ВолГУ, 2013. С. 71–78.
9. Масленников Д. Развитие информационных угроз в первом квартале 2013 г. [Электронный ресурс] // Лаборатория Касперского. Аналитика от 15 мая 2013 г. URL: http://www.securelist.com/ru/analysis/208050801/Razvitie_informatsionnykh_ugroz_v_ pervom_kvartale_2013_goda (дата обращения 15.10.2013).
10. Никишова А.В. Кооперация агентов многоагентной системы обнаружения атак // Актуальные вопросы информационной безопасности регионов в условиях глобали- зации информационного пространства. Матер. II Всеросс. науч.-практ. конф., Волго- град, 26 апреля 2013 г. Волгоград: Изд-во ВолГУ, 2013. С. 118–120.
11. Никишова А.В. Архитектура типовой информационной системы для

задачи обна- ружения атак // Известия ЮФУ. Технические науки. 2011. № 12 (125). С. 104–109.

12. Платонов В.В. Программно-аппаратные средства защиты информации: учеб.для вузов по напр. подготовки «Информационная безопасность». М.: ИЦ «Академия», 2014. 331 с.

13. Партыка Т.Л., Попов И.И. Информационная безопасность: учеб.пособие. 5-е изд., перераб. и доп. М.: ИД «Форум»; НИЦ ИНФРА-М, 2016. 432 с.

14. Шаньгин В.Ф. Информационная безопасность компьютерных систем и сетей: учеб.пособие. М.: ИД «Форум»; НИЦ ИНФРА-М, 2014. 416 с.

15. McAfeeThreatsReport: SecondQuarter 2013 [Электронныйресурс] // McAfeeLabs. Reports.

16. URL: http://www.mcafee.com/ca/resources/reports/rp-quarterly-threat-q2-2013.pdf

17. Muller Jorg P.The Design of Intelligent Agents: a Layered Approach / Jorg P. Muller.

18. Berlin; Heidelberg; New York: Springer, 1996. Vol. 1177.

19. Shoham Y., Leyton-Brown K. Multiagent Systems: Algorithmic, Game-Theoretic, and Logical Foundations. NewYork: CambridgeUniversity, 2009.