«Аналітичні оцінки рівня захищенності розподілених і масштабованих систем»

Підготував:
студент групи КА-51
Дубінчук А.О.
Дипломний керівник:
професор Мухін В.Є.

Огляд літератури

- Кризис информационной безопасности - Режим доступу: https://studopedia.su/13_86560_krizis-informatsionnoy-bezopasnosti.html
- В.А. Мукминов, к.т.н.; В.М. Хуцишвили, к.т.н.; А.В. Лобузько МЕТОДИКА ОЦЕНКИ РЕАЛЬНОГО УРОВНЯ ЗАЩИЩЕННОСТИ АВТОМАТИЗИРОВАННЫХ СИСТЕМ / В.А. Мукминов, к.т.н.; В.М. Хуцишвили, к.т.н.; А.В. Лобузько - 4 ЦНИИ Минобороны России, г. Тверь, 2012
- Критерии определения безопасности компьютерных систем – Режим доступу: https://ru.wikipedia.org/wiki/%D0%9A%D1%80%D0%B8%D1%82%D0%B5%D1%80%D0%B8%D0%B8_%D0%BE%D0%BF%D1%80%D0%B5%D0%B4%D0%B5%D0%BB%D0%B5%D0%BD%D0%B8%D1%8F_%D0%B1%D0%B5%D0%B7%D0%BE%D0%BF%D0%B0%D1%81%D0%BD%D0%BE%D1%81%D1%82%D0%B8_%D0%BA%D0%BE%D0%BC%D0%BF%D1%8C%D1%8E%D1%82%D0%B5%D1%80%D0%BD%D1%8B%D1%85_%D1%81%D0%B8%D1%81%D1%82%D0%B5%D0%BC
- Способы защиты информации – Режим доступа: https://searchinform.ru/informatsionnaya-bezopasnost/zaschita-informatsii/sposoby-zaschity-informatsii/
- Системы мониторинга событий безопасности – Режим доступа: https://www.anti-malware.ru/security/security-monitoring - Дата доступа: 03.04.2019
- Методи оценок защищенности распределенных информационных систем – Режим доступу - http://tekhnosfera.com/view/51664/d#?page=1
- Криптографические методы защиты информации – Режим доступу: https://sites.google.com/site/anisimovkhv/learning/kripto/lecture/tema1
- Е.В. Дойникова Показатели и методики оценки защищенности компьютерных сетей на основе графов атак и графов зависимостей сервисов / Е.В. Дойнікова - Санкт-Петербургский институт информатики и автоматизации РАН, 2013
- Предметная область информационной безопасности – Режим доступа: https://works.doklad.ru/view/C8Pxf2nQ35M.html
- Сетевые атаки.Виды.Способы борьбы – Режим доступа: https://moluch.ru/conf/tech/archive/5/1115/

Актуальність задачі, що розглядається

- Дуже часто від безперебійної роботи комп’ютерних систем та постійного вільного доступу до інформації залежить надійність, якість та взагалі функціонування цілих організацій
- У зв’язку з цим виникає потреба в захисті цієї інформації, а також у аналізі захищеності комп’ютерної системи. Вже є розроблені стандарти означенню безпеки комп’ютерних систем, які впроваджуються на державному рівні. Одним з яскравих прикладів є «Критерії визначення безпеки комп’ютерних систем» («Оранжева книга»). Це стандарт прийнятий міністерством оборони США, який визначає основні умови для оцінки ефективності засобів комп’ютерної безпеки

Актуальність задачі, що розглядається

- Тож, на сьогоднішній день все більше і більше уваги приділяється захищеності даних та комп’ютерних систем про що свідчить встановлення правової бази та створення величезної кількості засобів оцінки захищеності, моніторингу захищеності, оцінки ризиків комп’ютерних систем. Захист інформації всередині комп’ютерної системи є однією з найважливіших задач, які вирішуються на сьогодні не тільки через важливість інформації, що вони містять, а й через постійне зростання кількості та якості методів та створення нових підходів до атак на комп’ютерні системи

Існуючі методи вирішення задачі

- На сьогоднішній день існує безліч програм за допомогою яких або за результатами роботи яких можна оцінити захищеність комп’ютерних систем. До них належать програмні засоби по пошуку вразливостей на відкритих портах даної комп’ютерної системи, системи моніторингу захищеності, сканери портів та так звані програми слухачі, які аналізують трафік, що йде через комп’ютерну систему.
- Щодо існуючих оцінок захищеності, то на даний момент немає єдиної розробленої методології та кожен дослідник пропонує свої. Серед найбільш часто використовуваних можна виділити такі, як знаходження слабкості порта відностно інших, CVSS оцінки, є оцінка мережевої захищеності, що розраховуються як кількість зафіксованих атак до загальної кількості проведених.

Поняття та класифікація загроз комп’ютерних систем

- Під загрозою інформаційній безпеці комп’ютерної системі будемо розуміти ті події, які є потенціально можливі, ті дії, процеси або явища, котрі здатні спричинити небажаний або ж визначений як атака вплив на комп’ютерну систему і інформацію, що в ній знаходиться.

Дерево класифікації загроз комп'ютерних систем

Найбільш поширені атаки

- Перехват паролів
- Переповнення буферу
- SQL/PHP-ін’єкція
- DoS- и DDoS- атаки
- phishing-атаки
- Атаки, що використовують електро-магнітну природу роботи КС

Постановка задачі дослідження

- В даній роботі я поставив собі задачу дослідити які є програмні засоби для оцінки захищеності комп’ютерної системи. Визначити як вони працюють, а саме, що приймають на вхід, які дають результати, і як скористатись цими результатами, що б дати системі оцінки захищеності.
- Також я маю дослідити існуючі оцінки захищеності, проаналізувати їх, використати, та, якщо треба вивести свої. Для цього я маю дослідити реальну систему на захищеність, шляхом знаходження її «характеристик», тобто портів, відкритих портів, вразливостей на цих портах, використати цю інформацію для знаходження оцінок.
- З отриманих результатів необхідно зробити висновок о захищеності комп’ютерної системи, яку я досліджував.

Використані програмних засобів для дослідження захищеності комп’ютерних систем

- Командна строка Windows, а саме її команда netstat –aon, для того, щоб побачити активні на час виклику команди IP-адреси
- Програмний засіб SuperScan, для того щоб знайти выдкриті порти на знайдених IP-адресах
- Nessus Vulnerability Scanner, для того, щоб знайти вразливості на портах та визначити їх CVSS оцінки.

Оцінки CVSS

- CVSS (Common Vulnerability Scoping System) – це оцінка, яка задається на інтервалі від 0 до 10, де 10 – це буде максимальний рівень небезпеки, що відповідає критичній вразливості, і визначає фактор ризику. Тобто за цією оцінкою ми можемо визначити критичність атаки на комп’ютерну систему.

Оцінки CVSS

- CVSS – це відкритий стандарт, і розраховується оцінка за наступною формулою:

$$\boldsymbol{CVSS = 10 \cdot AV \cdot AC \cdot Au \cdot ((C_1 \cdot C_2) + (I_1 \cdot I_2) + (A_1 \cdot A_2))}$$

- *AV* (Access Vector – вектор доступа), який дорівнює 0,7 в разі, якщо необхідно використовувати локальний доступ для використання вразливості, та 1, якщо можливе віддалене використання вразливості.
- *AC* (Access Complexity — важкість доступу і реалізації атаки):0,8 – висока, 1 – низька.
- *Au* (Authentication — аутентифікація): 0,6 — потрібна, 1 — непотрібна.
- C_1 (Confidentiality Impact – вплив на конфіденційність): 0 —відсутній, 0,7 — частково відсутній, 1 — може повністю порушити конфіденційність.
- I_1 (Integrity Impact — вплив на цілісність): 0 — відсутній, 0,7 — частково присутній, 1 — може повністю порушити цілісність;
- A_1 (Availability Impact — вплив на доступність): 0 — відсутній, 0,7 —
- частково присутній, 1 — може повністю порушити доступність;
- C_2, I_2, A_2 — коефіцієнти впливу загрози (Impact Bias) на конфіденційність, цілісність та доступність.

Оцінка захищеності локального тестування

$$L = 1 - \frac{\sum_{i=1}^{n} Y_i}{\sum_{i=1}^{n} P_i}$$

- P_i – кількість відкритих портів на і-м IP
- Y_i – кількість портів і-го IP, на яких була знайдена вразливість
- n – кількість тестуємих IP комп’ютерної системи.

Оцінка захищеності зовнішнього тестування

$$\boldsymbol{Z = \frac{1}{n} \sum_{i=1}^{n} Za_i}$$

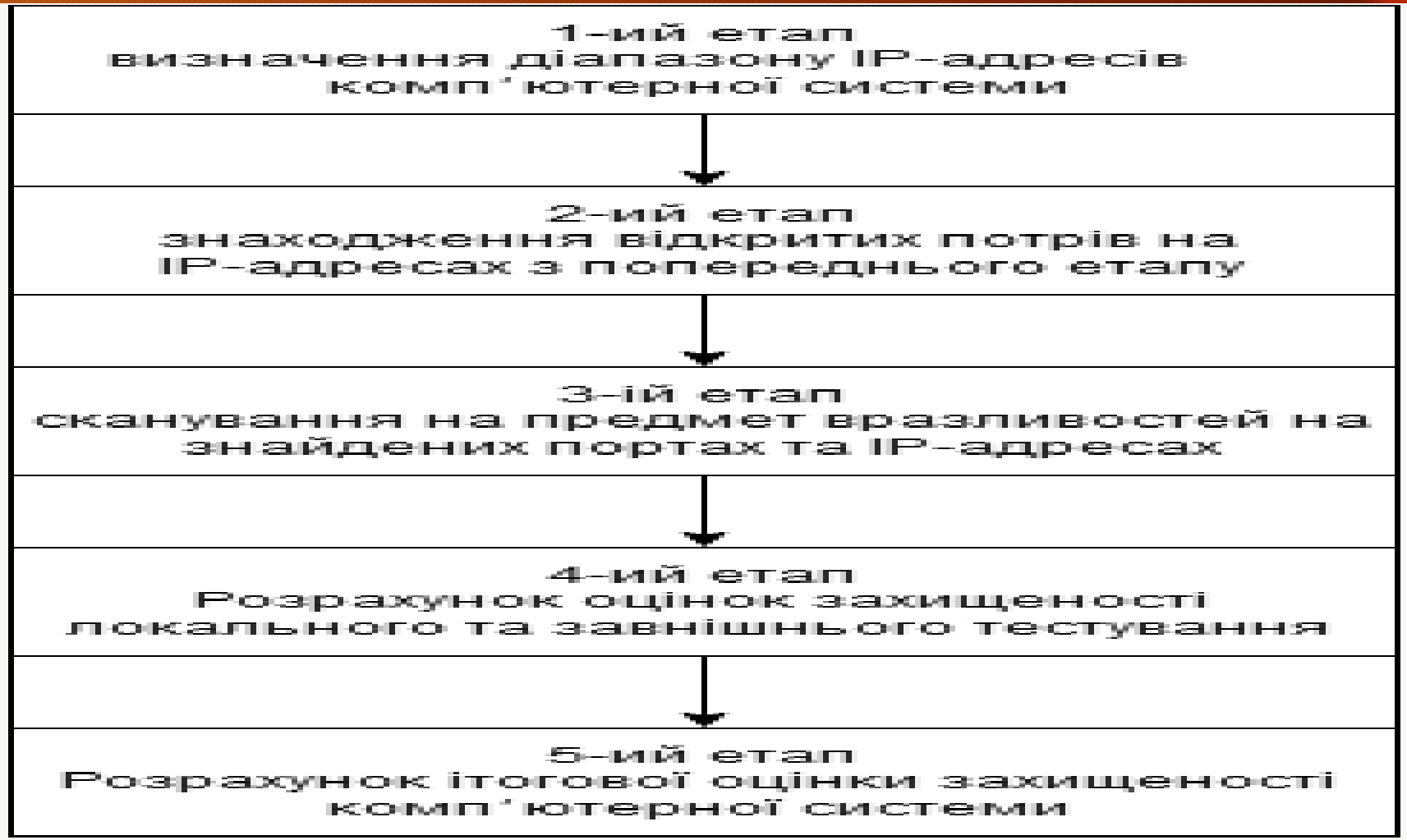
- $Za_i = \prod_{j=1}^{m_i}(1 - \frac{1}{10} CVSS_{ij})$ (2.3)
- m_i- кількість вразливостей на і-му хості
- $CVSS_{ij}$ - оцінка CVSS ні і-му хості для вразливості j
- Za_i - оцінка відбиття атаки/захищеності від атак на і-му хості

Ітогова оцінка захищенності системи

$$I = Z \cdot L$$

ітогова оцінка захищенності системи I за локальним та зовнішнім тестуванням(захищеність від атак), я їх добуток, бо приймається до уваги і локальна захищеність і зовнішня

Алгоритм розв’язку



Знайдені відкриті порти за допомогою програмного засобу SuperScan

IP-адрес	Відкриті порти
127.0.0.1	0, 135, 445, 554, 1688, 1947,3001, 49156
192.168.1.102	0, 135, 139, 445, 554, 1688, 1947, 49156
176.38.88.68	0, 25, 53, 80, 110, 119, 143, 465, 563, 587, 993, 995
176.38.88.1	0, 8, 445, 554, 1688, 2000
176.38.88.22	0, 80, 135, 554, 1688, 1947

Знайдені вразливості на портах задопомогою програмного засобу Nessus Vulnerability Scanner

IP-адрес	Уязвимість	Порт	$CVSS$	$\frac{1}{10}CVSS$	$1-\frac{1}{10}CVSS$
176.38.88.68	Є можливість перечислити імена CPE, які співпадають на віддаленій системі	tcp/0	1	0,1	0,9
	Можливість угадати тип віддаленого пристрою	tcp/0	1,2	0,12	0,88
	Веб-сервер запущений на віддаленому хості	tcp/80	0	0	1
	Можливо визначити ім'я віддаленого хоста	tcp/0	1	0,1	0,9
	Може бути витягнута інформація про віддалений HTTP	tcp/80	1,4	0,14	0,86
	Можливе визначення точного часу, встановленого на віддаленому хості	icmp/0	0	0	1
	Можливе визначення відкритого TCP-порту	tcp/53	1,8	0,18	0,82
127.0.0.1	На віддаленний хост Windows впливають багато вразливостей	tcp/455	8,1	0,81	0,19
	На віддаленому підвищена вразливість	tcp/49156	6,8	0,68	0,32
	Авторизація не потрібна на віддаленому сервері SMB	tcp/455	5,3	0,53	0,47
	Плагін збирає інформацію про віддалений хост через аутентифікований сеанс	tcp/0	1,3	0,13	0,87
	На віддаленому хості запущено службу DCE / RPC	tcp/135	1	0,1	0,9
192.168.1.102	На віддаленний хост Windows впливають багато вразливостей	tcp/455	8,7	0,87	0,13
	На віддаленому підвищена вразливість	tcp/49156	5	0,5	0,5
	Авторизація не потрібна на віддаленому сервері SMB	tcp/455	5	0,5	0,5
	На віддаленому хості запущено службу DCE / RPC.	tcp/49156	1,1	0,11	0,89

Знайдені вразливості на портах задопомогою програмного засобу Nessus Vulnerability Scanner

IP-адрес	Уязвимість	Порт	$CVSS$	$\frac{1}{10}CVSS$	$1-\frac{1}{10}CVSS$
192.168.1.102	Можна вгадати тип віддаленого пристрою.	tcp/0	0	0	1
	Виробник може бути ідентифікований з Ethernet OUI.	tcp/0	1,1	0,11	0,89
176.38.88.1	Можливо отримати інформацію про трасування	udp/8	0	0	1
	Можна визначити ім'я віддаленого вузла	tcp/0	0,8	0,08	0,92
	Можна визначити, які порти TCP відкриті	tcp/2000	1,8	0,18	0,82
	Віддалена служба реалізує мітки часу TCP	tcp/0	1,1	0,11	0,89
176.38.88.22	Можна визначити точний час, встановлений на віддаленому хості	icmp/0	0	0	1
	Можна визначити ім'я віддаленого вузла	tcp/0	0,9	0,09	0,91
	Створює traceroute до віддаленого хоста.	udp/0	1,2	0,12	0,88
	Веб-сервер запущений на віддаленому хості	tcp/80	0,1	0,01	0,99

Знаходження оцінки рівня захищеності компютерної системи

- $Za_{176.38.88.68} = \prod_{j=1}^{7}(1 - \frac{1}{10} CVSS_{176.38.88.68\ j}) = 0.9 \cdot 0.88 \cdot 1 \cdot 0.9 \cdot 0.86 \cdot 1 \cdot 0.82 \approx 0.5027$
- $Za_{127.0.0.1} = \prod_{j=1}^{5}(1 - \frac{1}{10} CVSS_{127.0.0.1\ j}) = 0.19 \cdot 0.32 \cdot 0.47 \cdot 0.87 \cdot 0.9 \approx 0.0224$
- $Za_{192.168.1.102} = \prod_{j=1}^{6}(1 - \frac{1}{10} CVSS_{192.168.1.102\ j}) = 0.13 \cdot 0.5 \cdot 0.5 \cdot 0.89 \cdot 1 \cdot 0.89 \approx 0.0257$
- $Za_{176.38.88.1} = \prod_{j=1}^{4}(1 - \frac{1}{10} CVSS_{176.38.88.1\ j}) = 1 \cdot 0.92 \cdot 0.82 \cdot 0.89 \approx 0.6714$
- $Za_{176.38.88.22} = \prod_{j=1}^{4}(1 - \frac{1}{10} CVSS_{176.38.88.22\ j}) = 1 \cdot 0.91 \cdot 0.88 \cdot 0.99 \approx 0.7923$

Знаходження оцінки рівня захищеності компютерної системи

- $Z = \frac{1}{5}\sum_{i=1}^{5} Za_i = \frac{1}{5}(0.5027 + 0.0224 + 0.0257 + 0.6714 + 0.7923) \approx 0.4029$
- $L = 1 - \frac{\sum_{i=1}^{5} Y_i}{\sum_{i=1}^{5} P_i} = 1 - \frac{(3+4+3+3+2)}{(12+8+8+6+6)} = 0.625$
- $I = L * Z = 0.625 * 0.4029 \approx 0.2518$

- Отже, можна зробити висновок, що тестуєма комп’ютерна система захищена дуже погано, і дуже вразлива до різного роду атак.

Висновок

- В ході дослідження було побачено, що є декілька типів програмних засобів, одні з яких сканують комп’ютерну систему на предмет вразливостей, в той час як інші безпосередньо проводять аналіз активних підключень та проводять оцінку можливих загроз від них. Також під час написання роботи було проаналізовано безліч різних оцінок захищеності. Вони відрізняються направленістю(локальне тестування та зовнішнє).
- Проте, в роботі було прийнято рішення використовувати власні оцінки, а не вже існуючі, через те, що на думку автора роботи оцінки приведені іншими дослідниками не є такими, що відображають захищеність або ж і взагалі не є математичними. В той же час приведені в роботі оцінки рівня захищеності використовують загально прийнятий стандарт по оцінці критичності атак CVSS.
- Потім був зроблений висновок, щодо реальності такої оцінки відповідно до існуючої картини, а також був зроблений висновок чому рівеньзахищеності є таким.
- Тож, можна зробити висновок, що приведені у роботі оцінки вигідно відрізняються від інших, виникших в ході дослідження даної теми, бо вони допомагають оцінити рівень захищеності комп’ютерної системи за двома напрямками, отримати ітогову оцінку, вони є математично вірними, та підходять до аналізу будь-яких комп’ютерних систем, тобто є універсальними.

Дякую за увагу