IT4Sec Reports 151
http://dx.doi.org/10.11610/it4sec.0151

Техники за оценяване на киберзаплахи в мрежови системи за управление

Николай Найденов Хранов

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
www.IT4Sec.org

София, юли 2023

Николай Найденов Хранов, Техники за оценяване на киберзаплахи в мрежови системи за управление, *IT4Sec Reports 151*(юли 2023), http://dx.doi.org/10.11610/it4sec.0151

IT4Sec Reports 151 „Техники за оценяване на киберзаплахи в мрежови системи за управление" В свят, в който хората са напълно зависими от компютърните технологии и информационните системи, защитата на информацията е от решаващо значение. В изследване е направен преглед на някои по-известни решения за техническо оценяване на киберзаплахите в рискова, „чувствителна“ информационна среда, а именно мрежови информационни системи на управление.

Ключови думи: Киберзаплахи, мрежови системи на управление техники за идентифициране/оценяване

IT4SecReports 151 "Evaluation techniques for cyber threats in network management systems" In a world where people are completely dependent on computer technology and information systems, the protection of information is of critical importance. The study presents an overview of some popular solutions for technical assessment of cyber threats in a risky, "sensitive" information environment, namely network management systems.

Keywords: Cyber threats, network management systems, identification/assessment techniques

ISSN 1314-2119

ВЪВЕДЕНИЕ

За целите на настоящето изследване са разгледани следните техники за оценка на мрежови информационни системи на управление:

Ръчни техники за изследване и оценка на системи, приложения, мрежи, политики и процедури, за откриване на слабите места. Включват документи, дневници, набор от правила, както и преглед на конфигурацията на системата, network sniffing и проверка на интегритета на файловете.

Техники за идентифициране на целите: Включват откриване на мрежа (network detection), мрежов порт и идентификация на услуга, сканиране на уязвимост, сканиране и проверка на сигурността на приложенията. Като за нуждите на настоящото изследване се извършват ръчно или с помощта на автоматизирани инструменти, като: Nessus и OpenVAS.

Пояснение на използваните инструменти:

Nessus: Представлява *Remote* одитор за мрежова сигурност, с инструмент Nessus Scanner. Чрез него е осъществено тестване на модули за сигурност в опит да бъдат открити уязвимите места в мрежови информационни системи на управление. Nessus се състои от две части: сървър и клиент. Сървърът / демон – nessusd, е отговорен за атаките, докато Nessus, ни предоставя резултатите от теста в графичен интерфейс [1].

OpenVAS означава *Open Vulnerability Assessment System* (система за оценка на уязвимости) и представлява мрежови скенер за сигурност. Състои се от сървър с набор от възможности и методи за тестване на уязвимости в отдалечени системи и приложения [2].

Продукта OpenVAS е безплатен софтуер под GNU GPL и клон на Nessus (визира се Corp. edition 4.2.x).

Използваните техники за валидиране на целевите уязвимости включват: penetration testing, социално инженерство, тестване на сигурността.

МЕТОДОЛОГИЯ НА ИЗСЛЕДВАНЕТО

Оценката за информационна сигурност изисква ресурси като време, персонал, хардуер и софтуер. Разработването на правилна методология за оценка на информационна сигурност дава възможност за намаляване на разходите чрез възможност за повторно използване на предварително определени ресурси (обучен персонал и стандартизирани платформи за тестване).

Методологията съдържа следните фази:

Планиране - Фазата на планиране се използва за събиране на информация кои активи да бъдат оценявани, определяне на заплахите срещу активите, както и проверки за сигурност, които да се използват за смекчаване на тези заплахи и да се развие подход за оценка. Оценката на сигурността трябва да бъде третирана като всеки друг проект, с план за управление на проекта, с целите и задачите, обхвата и изискванията, роли и отговорности, ограничения, фактори за успех, предположения, ресурси, график, и резултати.

Изпълнение - Основни цели за етапа е да се открият слаби места и да се валидират, когато е необходимо. След приключване на тази фаза оценителите ще са идентифицирали системата, мрежата и уязвимости.

Фаза „след изпълнение“ се фокусира върху анализ на установените уязвимости, за да определи основните причини, препоръки за смекчаване на въздействието и окончателен доклад.

Използвани техники за преглед на мрежови информационни системи на управление:

Техниките за преглед представляват пасивно изследване на системата, приложенията, политиките и процедурите, за откриване на слаби страни в сигурността.

Установени са следните технически похвати в Таблица 1, както следва:

Таблица 1. Основни способности на използваните техники.

Техника	***Способности***
Преглед на логовете (информационният журнал)	Предоставя историческа информация за употребата на системата, конфигурацията, промените. Може да разкрие потенциални проблеми и недостатъци на системата
Преглед на набора от правила	Разкрива пропуски в набора от правила за сигурност
Преглед на конфигурацията на системата	Оценява надеждността на конфигуриране на системата. Удостоверява, че системата е конфигурирана в съгласие с установените политики.
Подслушване на мрежата / sniffing	Прави се мониторинг на трафика на определен сегмент, за прихващане на информация за операционна система, комуникационни протоколи, услуги, приложения Потвърждава криптирането на комуникацията
Проверка интегритета на файловете	Показва промените във важни файлове, идентифицира нежелани файлове

РЕЗУЛТАТИ

При идентифициране на потенциална цел и прилагане на аналитични техники, се акцентира върху идентифициране на активни устройства и техните отворени портове и услуги и анализиране на потенциалните им слабости. Създаден е модел за анализиране.

Откриване на мрежи

Съществуват активни и пасивни техники за откриване на устройствата в мрежата. Пасивните техники използват мрежови снифър (sniffer) за наблюдаване на трафика в мрежата, записване на IP адреси на активни хостове, какви операционни системи са открити в мрежата. Пасивното търсене може също така да разкрие каква е връзката (relationship) между хостовете – включително кой хост с кой комуникира, колко често се случва тяхната комуникация и какъв тип трафик има между тях – това обикновенно се случва от хост от вътрешната мрежа където той може да следи връзките между различните хостове. Това се прави без изпращане на пробен пакет (probing packet). Пасивното търсене има нужда от повече време за събиране на информация отколкото активно търсене.

Идентифициране на мрежови портове и услуги

Идентифицирането на мрежови портове и услуги включва използването на портови скенер, за да се идентифицират мрежовите портове и услуги които работят на активният хост – като ftp и http/https – и приложенията, които ползват всяка идентифицирана услуга, като Microsoft Internet Information Server (IIS) или Apache за http/https услугите. Компаниите би трябвало да провеждат идентификация на мрежови портове и услуги за да откриват хостове, ако това не е направено вече чрез други средства (като откриване на мрежи), и за да посочат потенциални уязвими услуги. Тази информация се използва за да се определят цели за пенетрейшън тестинг.

Сканиране за уязвимости

Сканирането за уязвимости идентифицира хостове и хостовите атрибути (например, операционни системи, приложения, отворени портове), но също така се опитва да идентифицира уязвимости.

Чрез сканиране за уязвимости могат:

- Да следят за използваните услуги от хоста и спазването на политиките за сигурност.
- Да предоставят информация за целта за penetration testing.
- Да предоставят информация как да се намали ефекта от откритите уязвимости.

Сканирането за уязвимости е сравнително бърз и лесен начин да се определи количествено експозицията на дадена организация към повърхностни уязвимости (surface vulnerabilities). Повърхностната уязвимост е слабост, която съществува в изолация, независимо от други фактори за уязвимост. Поведението и изходните данни, предоставени от скенера, на системата в отговор на атака, се сравняват с тези, които се характеризират с подписите (signatures) на известни уязвимости и инструментът докладва всички съвпадения, които са намерени. Освен сканиране на базата на подпис, се симулират модели за разузнаване като скенера използва сонда за открити уязвимости, и докладва когато тези техники са успешни.

Поставяне на Техники за валидиране на целеви уязвимости на мрежови информационни системи на управление

Валидиране на целеви уязвимости се извършва на основание на информацията получена от идентифициране и последващо анализиране на потенциални уязвимости. Валидирането на целевите уязвимости носи значително количество риск, тъй като тези техники имат повече потенциал да влияят върху целевата система или мрежата отколкото другите техники, според „Техническо ръководство за тестване и оценяване на информационна безопасност”, разработено от Националният институт за стандарти и технологии (NIST) [3].

Провеждане на Penetration Testing

Penetration Testing е тест за сигурност, при който експертите симулират атаките от реалния свят, с помощта на инструменти и техники, които обикновено се използват от хакерите за да идентифицират уязвимости в защитните функции на приложението, системата или мрежата. Penetration Testing включва търсене на комбинации от уязвимости.

Ползи от Penetration Testing:

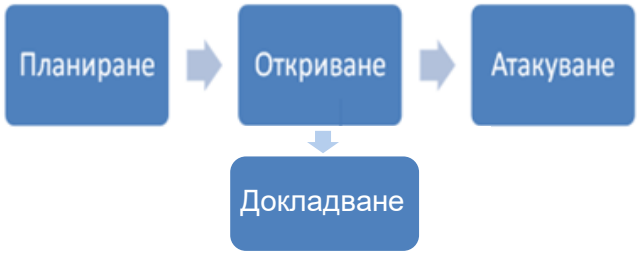
- Определяне колко добре системата толерира модели на атаки в реалния свят.
- Най-вероятното, необходимо ниво компетентност на атакуващия за успешна атака.

- Допълнителни мерки за противодействие, които биха могли да смекчат заплахите срещу системата.
- Способността на защитниците за откриване на атаките и адекватно реагиране.

Нетехнически методи за Penetration Testing:

- нарушаване на контрола на физическата сигурност и процедурите за свързване към мрежата;
- откradване на оборудване, придобиване на чувствителна информация (чрез инсталиране на Keylogging устройства)
- нарушаване на комуникация;
- социален инженеринг;

Установени фази на Penetration Testing. Съгласно Фигура 1 са представени четири фази на Penetration Testing.



Фиг. 1. Фази на Penetration testing.

Фаза „Планиране“:

- Определят се правилата и целите
- Финализира се и се документира одобрението на ръководството
- Фактическото тестване не се извършва в тази фаза

Във Фаза „Откриване“ са включени две части, свързани с „Докладването“:

Началото на действителното изпитване, което обхваща събирането на информация и сканирането. Провежда се Network port идентификация на услугите, за да се идентифицират потенциални цели. В допълнение се използват други техники за събиране на информацията за целевата мрежа:

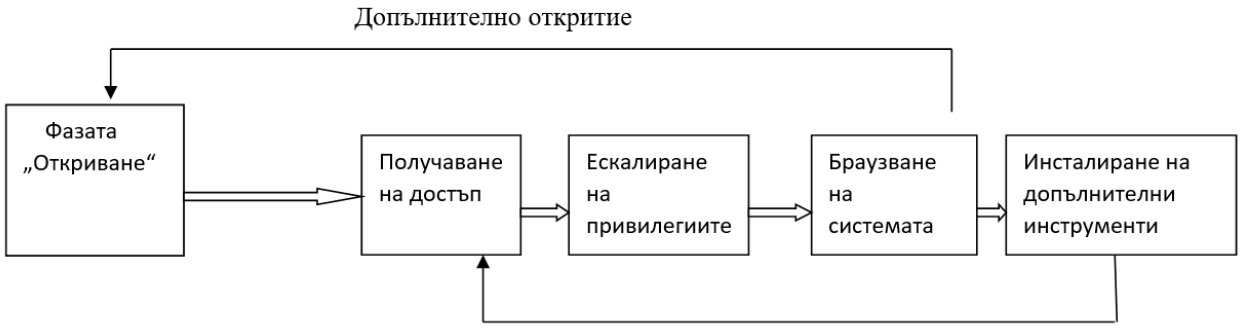
- Host name и информация относно IP адреса. Може да бъде придобита по много начини, включително DNS interrogation, InterNIC (WHOIS) заявки и мрежов снифинг (основно само по време на вътрешно тестиране).
- Имената и контактната информация на служителите може да бъде получена чрез търсене в уеб-сървърите на организацията или сървър за директорийни услуги.
- Системна информация, като имена и споделяния могат да бъдат намерени чрез методи като NetBIOS изброяване (обикновено само по време на вътрешни тестове) и мрежова информационна система (NIS) (обикновено само по време на вътрешни тестове).
- Информация относно услуги и приложения, като например номерата на версиите, може да бъде намерена с помощта на банер.

В някои случаи техниките, като dumpster diving и физически достъп до съоръженията може да се използва за събиране на допълнителна информация за целевата мрежа (например пароли, написани на хартия).

Във втората част на фазата „Откриване“ - анализ на уязвимостите, което включва сравняване на сканираните услуги, приложения и операционни системи с тези в базата данни и собствените знания на Penetration test операторите.

Ръчно търсене на уязвимостите е по-бавно, но помага за идентифицирането на нови или неизвестни уязвимости, които автоматизираните скенери могат да пропуснат.

Фаза „Атакуване“ (Фиг. 2). Представлява проверка на предварително идентифицираните потенциални уязвимости, опит за експлоатирането им, ескалиране на привилегиите на Penetration test операторите с цел получаване на достъп до допълнителни ресурси в системата или мрежата.



Фиг. 2. Фаза “Атакуване“.

Получаване на достъп - Използване на данните от етап „Откриване“, за да се направи информиран опит за достъп до целевата система.

Ескалиране на привилегиите - само ако на предишната стъпка се получи достъп до системата, изпитващия ще се опита да получи пълен контрол над системата (администраторски права).

Браузване на системата - Процеса на придобиване на информация за системата отново започва, за да се идентифицират механизми за придобиване на достъп до допълнителни системи.

Инсталиране на допълнителни инструменти - Допълнителни инструменти за проникване се инсталират с цел придобиване допълнителна информация и/или допълнителен достъп.

Категории уязвимости, експлоатирани от Penetration Testing

- *Неправилно конфигуриране.* Неправилно конфигурираните настройки за сигурност, особено тези по подразбиране, обикновено са лесно използваеми.
- *Kernel Flaws.* Kernel е ядрото на една операционна система, и представлява цялостния модел на сигурност на системата, така че всеки пропуск на сигурността в ядрото поставя цялата система в опасност.
- *Buffer Overflows.* Препълване на буфера се случва, когато програмите не проверяват адекватно на входа дали дължината е подходяща. Когато това се случи, в системата може да бъде въведен и изпълнен с привилегии (най - често

административни права) произволен код за административно ниво на изпълнение на програмата

- *Недостатъчно валидиране на входа.* Много от приложенията не успяват да валидират напълно входните данни, които получават от потребителите. Един пример е уеб приложение, което вгражда заявените стойности от един потребител в базата данни. Ако потребителят въведе SQL команди вместо или в допълнение към исканата стойност и уеб приложението не филтрира SQL команди от заявката, може да се извършат зловредни промени, които потребителят да зададе и да причини това, което е известно, като SQL injection attack.
- *Symbolic Links.* Символична връзка е файл, който сочи към друг файл. Операционната система включва програми, които могат да променят правата за дадения файл. Ако тези програми се изпълняват с привилегировани права, потребителят може да създаде стратегически символични връзки, за да „подлъгва“ тези програми (да извършва желани промени) или да ги включва в списъка на критични системни файлове.
- *File Descriptor Attacks.* File descriptors са числа използвани от системата, за да се следи пътя на файловете вместо имената на файловете.
- *Race Conditions.* Състезателни условия могат да възникнат по време на въвеждане на програма или процес в режим „привилегия“. По време на атака потребител може да се възползва от по-високи привилегии, докато процеса или програмата са още в привилегирован режим.
- *Грешни права върху файлове и директории.* Неподходящи права могат да позволят много типове атаки, включително писане и четене на файловете с пароли или допълнения към списъка доверени отдалечени хостове.

Фазата „Докладване“ - възниква едновременно с другите фази на Penetration Test. Доклада обикновено описва идентифицираните уязвимости, представя рисков рейтинг и предоставя ръководство как да се смекчат откритите слабости.

Penetration Testing Logistics

Сценарият е проектиран така, че да симулира вътрешна и външна атака. В настоящето изследване за мрежови информационни системи на управление се използват вътрешни и външни методи за тестване.

„Аутсайдер сценарият” симулира външен нападател, който има малко или никакво специфично знание за целта и който работи изцяло на предположения. За да се симулира външна атака, изпитващите са снабдени с някаква реална информация за целевата среда (различна от целеви IP адреси или мрежи) от отворени източници (обществени уеб страници, дискусионни групи и други подобни). Сканираните портове и уязвимости се използват за идентифициране на целеви хостове. Тъй като трафика на изпитващия минава през защитна стена количеството на информацията получена от сканирането е много по-малко отколкото ако теста е предприет отвътре. След идентифициране на хостове в мрежата, които могат да бъдат достигнати от отвън, изпитващите се опитват да компрометират един от хостовете. При успех този достъп може да бъде използван за компрометиране на други хостове, които обикновено не могат да бъдат достъпени от външна страна на мрежата. Penetration testing е един повтарящ се процес, която използва минимален достъп за получаване на по-голям достъп.

„Вътрешният сценарии” симулира действия на зловредна вътрешна намеса, изпитващия се намира вътре в мрежата и притежава определени възможности за достъп към мрежата или системата. Използвайки този достъп, изпитващия се опитва да ескалира своите привилегии. Изпитващите са снабдени със стандартно ниво на достъп и информация

(работниците и служителите), въпреки че в зависимост от целите на теста това може да бъде информация, притежавана от мрежов администратор.

Penetration testing представлява висок риск за мрежите и системите на организацията, тъй като използва истински действия и атаки срещу производствени системи и данни. Поради високата си цена и потенциален риск, провеждането на Penetration testing може да бъде ограничено до веднъж годишно. Също така Penetration testing може да бъде спрян, ако изпитващия достигне точка, когато допълнително действие ще доведе до увреждане. Резултатите от теста трябва да бъдат взети под внимание насериозно, а откритите уязвимости да бъдат отстранени. Резултатите трябва да бъдат представени на ръководството.

Една добре проектирана програма за редовно насрочено сканиране на мрежата и уязвимостите, съчетани с периодичен Penetration testing, може да предотврати много видове атаки.

План за оценка

Планът за оценка предвижда структура и отчетност чрез документиране на планираните дейности за оценка, заедно с друга свързана информация . NIST SP 800 - 53A, осигурява допълнителна информация относно плана за оценка.

Планът за оценка следва да отговори на тези основни въпроси:

- Какъв е обхватът на оценката?
- Кой е упълномощен да проведе оценяването?
- Какви са логистиката оценката си?
- Как трябва да се обработват чувствителни данни?
- Какво би трябвало да възникне в случай на инцидент?

ЗАКЛЮЧЕНИЕ

Извършване (изпълнение) на оценката на сигурността на мрежови информационни системи на управление става на няколко етапа: *координация, оценяване, анализ, работа с данни* (обработка, събиране, съхранение) и *дейности след тестовете*. Важно е да отбележим че съвременните мрежови системи за обработка на информацията включват все повече елементи с изкуствен интелект, което прави тяхната кибер защита доста по-съвършена, но същевременно поставя предизвикателства към злонамерените атаки, които също стават асистирани и интелигентни. Състезанието в бъдеще се очаква да бъде основно в самоеволюиращи системи с изкуствен интелект за кибер атаки и защити, с активното участие на човека, като регулиращ и обучаващ фактор.

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] “Tenable Nessus: The Global Gold Standard in Vulnerability Assessment Built for the Modern Attack Surface,” *Tenable*, www.tenable.com/products/nessus

[2] “Greenbone OpenVAS,” Open Vulnerability Assessment Scanner, Greenbone AG, http://www.openvas.org

[3] Karen Scarfone, Murugiah Souppaya, Amanda Cody and Angela Orebaugh, “Technical Guide to Information Security Testing and Assessment,” NIST Special Publication 800-115, September 2008, National Institute of Standards and Technology, https://www.researchgate.net/publication/329973439_NIST_Special_Publication_800-115_Technical_Guide_to_Information_Security_Testing_and_Assessment