НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

БАКАЛАВЪРСКИ ФАКУЛТЕТ
Програма: “ИНФОРМАТИКА“

РЕФЕРАТ

КУРС CSCB845 КОМПЮТЪРНА СИГУРНОСТ

ТЕМА: PENETRATION TESTING

Разработил
/Симеон Кирилов Геловски/
Факултетен номер: F95506

Ръководител
/С. Торбов/

София, 2023 г.

СЪДЪРЖАНИЕ

УВОД

В днешно време, когато информационната сигурност става все по-значима и заплахите от кибератаки растат, организациите трябва да се предпазват и да гарантират, че техните системи и данни са сигурно защитени. Една от важните практики за подобряване на сигурността е Penetration Testing, познат още като етичен хакинг или тестове на проникване.

В резултат на пенетрационния тест, организацията получава ясна представа за своите слабости и рискове, които могат да бъдат злоупотребени от нападатели. Тестването позволява на организацията да предприеме необходимите стъпки за подобряване на сигурността, като поправя уязвимостите и въвежда по-ефективни мерки за защита.

Penetration Testing не само помага за предотвратяване на потенциални кибератаки, но и помага на организациите да се съобразят със законодателството и регулаторните изисквания. Тестовете могат да допринесат за спазването на стандарти за сигурност, като например PCI DSS (Payment Card Industry Data Security Standard), GDPR (General Data Protection Regulation) и други.

В светлината на неотложната необходимост от подобряване на информационната сигурност и намаляване на рисковете от кибератаки, тестовете за пробив стават неотменим инструмент за организациите. В настоящия реферат ще се разгледат различни аспекти на Penetration Testing, включително видове тестове, етапи на изпълнение, предимства и резултати.

КАКВО ПРЕДСТАВЛЯВА PENETRATION TESTING?

Penetration Testing представлява процеса на активно оценяване на сигурността на информационна система, мрежа, данни или приложение. Те симулират реални атаки, които могат да бъдат предизвикани от външни хакери, злонамерени служители, кибер-престъпни организации и др. Това е един контролиран процес, който се провежда според изискванията и ИТ обкръжението на дадена организация и след конкретна оторизация, като по никакъв начин не нарушава работоспособността на проверяваните системи и целостта на данните в тях. Целта е откриване на потенциални уязвимости и слабости в системата.

ОТ КОГО СЕ ИЗВЪРШВАТ ТЕСТОВЕТЕ ЗА ПРОНИКВАНЕ?

Тестовете за проникване се извършват от специалисти в областта на информационната сигурност, наречени пентестъри или етични хакери. Тези професионалисти са обучени да разбират сложността на информационната сигурност и да извършват контролирани атаки върху системи, мрежи и приложения.

Пентестърите обикновено имат широк спектър от знания и умения, включително познания в области като компютърна мрежа, операционни системи, уеб приложения, бази данни и криптография. Те разполагат със специализирани инструменти и методики

за извършване на пенетрационни тестове и са запознати с актуалните техники на атака и защита.

Пентестърите могат да бъдат вътрешни служители на организацията, които имат задачата да тестват и подобряват сигурността на вътрешни системи и мрежи, но най-добре е pen testing-а да бъде извършен от някого с малко или никакви предварителни познания за това как е защитена системата, тъй като той може да успее да разкрие слепи зони, пропуснати от разработчиците, които са я създали. Някои от най-добрите етични хакери са самоуки, като всъщност някои са реформирани престъпни хакери, които сега използват своя опит, за да помогнат за отстраняването на пропуски в сигурността, вместо да ги използват. Най-добрият кандидат за извършване на теста може да варира значително в зависимост от целевата компания и какъв тип тест се изисква да се инициира.

Важно е да отбележим, че пентестърите, независимо дали са вътрешни или външни специалисти, трябва да спазват етични и правни принципи по време на изпълнението на тестовете. Те трябва да работят с разрешението и съгласието на собствениците на системите и приложенията и да използват своите умения и знания само за целите на подобряване на сигурността и защита от външни заплахи.

КОГА СЕ ПРОВЕЖДАТ ТЕСТОВЕТЕ ЗА ПРОНИКВАНЕ?

Тестовете за проникване могат да се провеждат в различни сценарии и на различни етапи в жизнения цикъл на системата или приложението, като е препоръчително да се извършват поне веднъж годишно или всеки път в следните случаи:

1. При извършени промени по ИТ инфраструктура на дадена система: Всяка промяна в системата, като актуализации на софтуера, промени в мрежовата инфраструктура или добавяне на нови функции, може да доведе до потенциални уязвимости. Тестовете за проникване след промените помагат да се уверим, че няма нови рискове, които да се появят вследствие на промяната.
2. При въвеждането на нови системи в експлоатация: Тестовете за проникване могат да се изпълнят преди внедряването на нова система, мрежа или уеб приложение. Това позволява да се открият потенциални уязвимости и слабости преди системата да бъде пусната в продукция.
3. При поява на неочакван инцидент: При заподозрени или реални кибератаки или инциденти, пенетрационните тестове могат да бъдат изпълнени, за да се установи обхвата и последиците от нарушението, както и да се открият допълнителни уязвимости, които могат да бъдат злоупотребени.
4. При извеждането на приложения и системи за ползване от по-широк кръг потребители.
5. При промени в законодателството и регулаторните изисквания: Ако се въвеждат нови закони, регулации, свързани с информационната сигурност и защита на данните, стандарти като ISO 27001, PCI-DSS и др., пенетрационните тестове могат да помогнат на организацията да се съобрази с тези изисквания и да установи съответствието си с новите норми.

ЕТАПИ

Тестването на сигурността минава през няколко основни етапа, които най-общо казано са пет на брой.

1. Планиране и разузнаване

Първият етап включва определяне на обхвата и целите на теста, включително системите, на които трябва да се обърне внимание и методите за тестване, които да се използват. Извършва се събиране на информация за целевата система, включително IP адреси, URL адреси, информация за архитектурата и други релевантни данни с цел да се разбере по-добре как работи дадената система и какви биха могли да бъдат нейните потенциални уязвимости. Установява се комуникация със собствениците на системата или приложението, съгласуват се срокове, разрешения и други детайли, свързани с изпълнението на теста.

2. Сканиране

Вторият етап е Сканиране. Основата цел тук е да се разбере как приложението реагира на различни опити за проникване. Има два подхода, а именно чрез „Статичен анализ“ или „Динамичен анализ“. При статичния кодът на приложението се проверява, за да се оцени начинът, по който се държи той, докато работи. При този подход може да се сканира целият код на един пас. При динамичния подход проверката се прави в работещо състояние. Това е по-практичният начин, тъй като той може да оцени производителността на приложението в реално време. Събраната информация се използва за изготвяне на "картина" на целевата система, включваща потенциални точки на уязвимост и слабости.

3. Получаване на достъп

При третия етап се използват различни техники за атаки като cross-site скриптове, SQL injection, задкулисие (backdoors), социален инженеринг, фишинг и други методи. Целта на този етап е да се получи контрол и достъп до системата или приложението, използвайки откритите уязвимости или слабости.

4. Поддържане на достъп

Целта на този етап е да види дали тези уязвимости могат да бъдат използвани, за да се установи постоянно присъствие в системата или по-скоро достатъчно дълго, така че хакерът да може да си гарантира постоянен достъп. Идеята е да се имитират по-сложни постоянни заплахи, които често остават в системата с месеци, за да успеят за това време да откраднат най-чувствителната информация, с която приложението разполага.

5. Анализ

Резултатите от теста се обобщават и се изготвя доклад, който подробно описва всички специфични уязвимости, които са били използвани, чувствителни данни, до

които е имало достъп и времето, през което тестерът е успял да остане незабелязан в системата.

Тези етапи представляват общата рамка на пенетрационното тестване, като подробностите и методологиите могат да варират в зависимост от организацията и контекста на теста.

ВИДОВЕ

External testing

Този тип тестове биват насочени към информация, която е видима отвън за компанията: самото уеб приложение, уеб сайт на компанията, електронна поща, DNS сървъри. Целта е да се идентифицират възможности за проникване и уязвимости, достъпни от интернет, като например отворени портове, слаби конфигурации на сървъри, уязвими уеб приложения и други рискове.

Internal testing

Този вид тестване се изпълнява от вътрешния мрежови периметър на организацията, обикновено от локалната мрежа, зад firewall-а на приложението и симулира атака от злонамерен вътрешен човек. Разбира се, това не е непременно служител от компанията, а по-скоро служител, чиито данни са били откраднати с помощта на фишинг атака. Целта е да се провери сигурността на вътрешните системи, уязвимости, свързани с неправилна конфигурация, слаби пароли, недостатъци в управлението на достъпа и други подобни рискове.

Blind testing

При Blind testing или closed-box testing на тестерът се дава само името на предприятието, чиято система ще се тества, без никаква друга основна информация. Този тип тест предоставя на софтуерните екипи симулация в реално време как злонамерена заплаха влиза в системата.

Double-blind testing

При този подход се симулира готовността на организацията за атака, тъй като екипът по сигурността няма представа дали тестът за проникване е извършен правилно. Това също означава, че експертите по сигурността нямат време да се възползват, за да укрепят защитите си преди пробивът на данните - подобно на реалния сценарий за атака. Този тип тестване може да помогне да се тества мониторингът на сигурността на организацията, идентифицирането на инциденти и процедурите за реакция.

Targeted testing

При този сценарий както тестерът, така и служителите по сигурността работят заедно и се следят взаимно за своите движения. Това е ценно упражнение за обучение, което предоставя на екипа по сигурността обратна връзка в реално време от гледната точка на един хакер.

Physical testing

Тук специалистите по киберсигурност се опитват да намерят „физически заплахи", което означава всяка атака, която може да бъде симулирана и включва физически местоположения. Може да включва разбиване на брави, кражба на устройства или използване на социална дейност, за да убеди служител да пусне хакери в сървърна стая. Полезно е да се разкрият слаби физически бариери и уязвимости на физическата сигурност като защитени процедури, които не се спазват, неработещи аларми за проникване, пропуски в оградите или дори проверка на охраната.

Това са само някои от основните видове пенетрационно тестване, като в практиката могат да се комбинират различни подходи и методи в зависимост от специфичните нужди и цели на организацията.

PEN TESTING VS WEB APPLICATION FIREWALL

Тестовете за проникване и WAF са самоизключващи се, но взаимно изгодни мерки за сигурност. За много видове pen testing (с изключение на blind и double blind тестовете) е вероятно тестерът да се възползва от WAF данни като регистрационни файлове, за да открие и използва слабите места на системата. В същото време WAF предлага активна защита срещу познати атаки и може да предотврати успеха на много общи такива. Използването на двете техники в комбинация може да предостави по-широка и по-ефективна сигурност.

ПЛЮСОВЕ И МИНУСИ

Предимства

Открива дупки в практиките за осигуряване на сигурност нагоре по веригата като автоматизирани инструменти, стандарти за конфигуриране и кодиране, анализ на архитектурата и други по-леки дейности за оценка на уязвимостта.

Намира както известни, така и неизвестни софтуерни пропуски и уязвимости в сигурността, включително малки, които сами по себе си няма да предизвикат голям проблем, но биха могли да причинят материални щети като част от сложен модел на атака.

Може да атакува всяка система, имитирайки начина, по който биха се държали повечето злонамерени хакери, симулирайки възможно най-близко ситуацията с такава каквато би била в реалния свят.

Недостатъци

Един от най-основните недостатъци е, че изпълнението на тестове за проникване е трудоемко и доста скъпо.

Може да има риск от нарушаване на достъпността на системата или приложението, особено ако процесът не се извършва правилно или се използват агресивни методи. Това може да предизвика прекъсване на работата или недостъпност за потребителите.