Уязвимости и атаки

Уязвимостта е податливост или недостатък на системата. Уязвимост съществува, когато съществува най-малко едно работещо нападение или експлойт.

За да се подсигури една компютърна система, е важно да се разберат атаките, които могат да се направят срещу нея. Тези заплахи могат да се класифицират в една от следните основни категории.

Подслушване

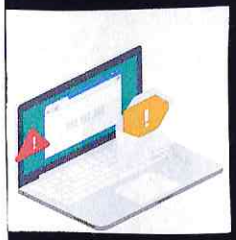
Подслушването е акт на тайно слушане на частен разговор, обикновено между хостове в една мрежа. Например, програми като Carnivore и NarusInsight се използват от ФБР и Агенцията за национална сигурност за подслушване на системите на доставчиците на интернет услуги. Дори машини, които работят като една затворена система могат да се подслушват чрез мониторинг на електромагнитните полета, генерирани от хардуера; TEMPEST е спецификация от НОБ, отнасящи се до тези атаки.

„Задни врати“

„Задна врата“ в компютърните системи, е всяка криптосистема или алгоритъм, които тайно заобикалят нормалните контроли за проверка на автентичността или сигурността. Те могат да съществуват поради различни причини. Те могат да бъдат добавени от оторизираната страна, с цел да позволи законен достъп или от нападател за злонамерени причини, но независимо от мотивите за тяхното съществуване, те са предпоставка за уязвимост.

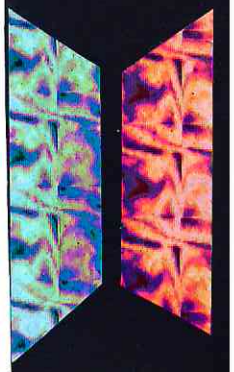
„Denial-of-service“ атаки

DoS атаките са проектирани да направят една машина или мрежов ресурс недостъпни за потребителите. Нападателите могат да спрат обслужването на отделни жертви, като например чрез умишлено въвеждане на грешна парола достатъчно последователни пъти предизвикващо блокиране на жертвата, или те могат да пренатоварят една машина или мрежа и да блокират всички потребители едновременно. Докато мрежовата атака от един IP адрес може да бъде блокирана чрез добавяне на ново правило в защитната стена, много форми на „Distributed denial of service“(DDoS) атаки са възможни, когато атаката идва от голям брой точки. Подобни атаки могат да произхождат от зомби компютрите на „Botnet“, но и редица други техники са възможни.



Фишинг

Фишинг е опитът да се придобие чувствителна информация като потребителски имена, пароли и информация за кредитни карти директно от потребителите. Фишингът обикновено се осъществява чрез имейл фишинг или мигновени съобщения, и то често насочва потребителите към въвеждане на данните в един фалшив уебсайт, чийто външен вид и усещане са почти идентичен с истинския.



Други

„Spoofing“

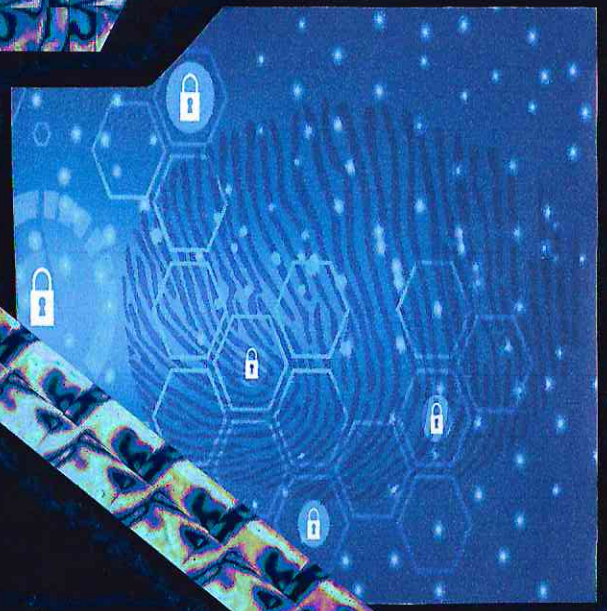
„Spoofing“ е техника, при която един човек или програма успешно се представя за друг чрез фалшифициране на данни.

„Нарушаване на целостта“

Зловредна модификация на продукти. Така наречените „Evil Maid“ атаки и охранителни услуги за наблюдение в рутери са пример за тях.

„Ескалация на привилегии“

Ескалацията на привилегии описва ситуация, в която един хакер с някакво ниво на ограничен достъп е в състояние да, издигне своите привилегии или ниво на достъп, без разрешение. Така например стандартен потребителски компютър може да бъде в състояние да заблуди системата, което дава достъп до ограничени данни или дори до пълен неограничен достъп до системата.



МОТИВИ ЗА АТАКИ

Както и при физическата сигурност, мотивациите за нарушения на компютърната сигурност, варират между нападателите. Някои от тях са търсачи на силни усещания или вандали, други са активисти или престъпници търсещи финансова изгода. Държавно-спонсорираните нападателите са често срещани и добре снабдени с информация, но в началото е имало аматьори като Markus Hess които хакнал КГБ.Стандартна част от модела за заплахи за всяка конкретна система е да се определи какво може да мотивира атака срещу тази система, и кои биха могли да бъдат мотивирани да го направят. Нивото и детайлността на предпазните мерки, варира в зависимост от системата. Домашен персонален компютър, банкови и секретни военни мрежи всички се сблъскват с много различни заплахи, дори когато свързаните с тях технологии, които се използват, са сходни.

“В бъдещето войните няма да бъдат водени от войници с оръжие или чрез самолети бомбардировачи. Война ще се започва с едно щракване на мишката на другия край на света, отприщвайки внимателно превърнати в оръжие компютърни програми, които нарушават или унищожават критични индустрии като комунални услуги, транспорт, комуникации и енергетика. Подобни атаки биха могли също така да деактивират военни мрежи, които контролират движението на войски, пътят на реактивни изтребители, командването и контролът на военни кораби.”

БЕЗОПАСЕН ИНТЕРНЕТ