ЗАШТИТА ПОДАТАКА

ЗАШТИТА СИСТЕМА

Улъези

Преглед

- Биће објашњено:
  - Улъези
  - Технике упада

Уљези

- Једна од две најпознатије претње по безбедност система су уљези, који се популарно називају и хакери (друга би били вируси).
- У почетку изучавања уљеза, примећене су три класе уљеза:
  - **Masquerader** - појединац који није овлашћен да користи рачунар и који пробија приступне контроле система да би користио легитиман кориснички налог
  - **Misfeasor** - легитимни корисник, који приступа подацима, програмима или ресурсима, за које такав приступ није дозвољен, или који је ауторизован за такав приступ али злоупотребљава своје привилегије
  - **Clandestine user** - појединац који заузима супервизорску контролу система и користи такву контролу да избегне бележење својих поступака (auditing) и контроле приступа или да потисне колекцију забелешки о својим поступцима (audit collection)
- Прва класа је обично неко ко споља покушава упад, друга класа је обично неко ко изнутра злоупотребљава систем, а трећа класа може бити и неко споља, али и неко изнутра.

Уљези (2)

- Напади уљеза се простиру од безазлених, па до озбиљних напада на систем.
- Безазлене нападе изводе појединци који једноставно желе да истражују, док озбиљни напади подразумевају, покушаје да се приступа поверљивим подацима, било да се они читају или да се мењају, што је тежа варијанта, као и покушаје да се подрије систем.
- 90-их година догодила су се многа хапшења и суђења због хакерских напада, али и одузимање огромне количине података, па и саме компјутерске опреме.
- Многи су веровали да је ситуација оваквим мерама стављена под контролу.

Улъези (3)

- Међутим, далеко од тога да је ситуација била под контролом.
- На пример: група из Бел лабораторије (Bell Labs) је пријављивала константне упаде на њихове рачунаре путем интернета у дужем временском периоду са више различитих извора.
- Они су доживљавали следеће:
  - покушаје да се копира фајл са шифрама темпом који је превазилазио једно копирање дневно
  - сумњиве позиве удаљених процедура (remote procedure call (RPC)) темпом који је превазилазио један позив недељно
  - покушаје да се повеже на непостојеће "мамац" машине, барем сваке две недеље

Уљези (4)

- Безазлени уљези могу се још и толерисати, мада умеју да смање перформансе система у великој мери.
- Проблем је што се никада не може унапред знати да ли је неки уљез безазлен или представља озбиљну претњу по систем.
- Управо због тога, јавља се потреба, чак и код система који нису осетљиви, да се овај проблем исконтролише на неки начин.

Уљези (5)

- Пример који илуструје проблем, догодио се у једном рачунском центру са више од 12000 умрежених рачунара.
- Особље центра било је обавештено да је један од њихових рачунара коришћен за напад на рачунаре на другој локацији путем интернета.
- Пратећи активности, особље је открило да је умешано неколико спољних уљеза, који су проваљивали шифре на неколико рачунара.
- Особље је искључило погођене машине, запушило неке уочене сигурносне пропусте и наставило са нормалним радом.

Улъези (6)

- Они су претпоставили да се ради о безазленим улъезима.
- Међутим, неколико дана касније, један од менаџера локалног система открио је да су се напади наставили.
- Испоставило се да су напади софистицираније него што се претпоставило.
- Пронађени су фајлови који садрже на стотине “проваљених” шифара, укључујући и неке за велике, и наводно сигурне, серверске машине.
- Такође, једна од локалних машина употребљена је да се постави огласна табла за хакере (bulletin board), помоћу које су хакери међусобно комуницирали.

Уљези (7)

- Анализа ових напада показала је да су уствари постојале две групе хакера: софистицирани са темељним познавањем технологије и друга група ("пешадија"), који су само користили програме за упад, које су добијали.
- Овакав тимски рад комбиновао је два најозбиљнија оружја уљеза:
  - софистицирано знање начина за упад у систем и
  - спремност да се проведе велики број сати покушавајући различите технике упада у систем.

Уљези (8)

- Један од резултата растуће забринутости због упада у систем је настанак многобројних тимова за пружање помоћи рачунару у опасности (computer emergency response teams (CERTs)).
- Овакви заједнички тимови сакупљају информације о слабостима система и достављају их менаџерима тих система.
- Нажалост, хакери могу доћи и до садржаја CERT извештаја.
- У претходном примеру, испоставило се да су хакери развили програме који тестирају буквално сваку од слабости рачунара поменуту у CERT извештају, и чак иако само једна машина није одреаговала брзо на CERT упозорења, остајала је отворена за нападе.

Улъези (9)

- Поред тога што су направили програм за проваљивање шифара, хакери су покушали и да модификују део софтвера за логовање, тако да добијају информације о шифрама сваког корисника који се улогује на систем.
- Ово им је омогућило да имају огромну количину шифара за приступ, коју су постављали на "огласну таблу", коју су поставили на једној од машина-жртава и са које су "пешадинци" могли да преузимају све што им је потребно за нападе.

Технике упада

- Циљ уљеза је да добије приступ систему, или да повећа привилегије које има на систему.
- У општем случају, ово значи да уљез треба да дође до података који би требало да су заштићени.
- У неким случајевима, подаци су у форми корисничке шифре и ако уљез сазна шифру неког корисника, онда може да користи систем на исти начин као регуларни корисник.

Технике упада (1)

- Типично, систем мора да има фајл који повезује шифре са корисницима.
- Уколико такав фајл није заштићен, онда је лак посао доћи до приступа овом фајлу и дохватити шифре корисника.
- Фајл са шифрама може бити заштићен на један од два начина:
  - **једностраним (one-way) функцијама**
  - **контролом приступа**

Технике упада (2)

- Код **једностраних функција** систем чува само вредност функције базирану на корисничкој шифри. Када корисник унесе шифру, систем трансформише шифру и пореди је са сачуваном вредношћу. У пракси, систем обично изводи једносмерну трансформацију (нереверзибилну) у којој се шифра користи да генерише кључ за једносмерну функцију и у којој се производи излаз фиксне дужине (значајно због различитих дужина шифре).
- Код **контроле приступа** приступ фајлу са шифрама је ограничен на једног или мали број корисника.

Технике упада (3)

- Уколико је једна или обе од ових контрамера примењена, потребан је одређени напор да би се дошло до шифре.
- Неке од техника за долажење до шифри су:
  1. Покушати са предодређеним шифрама, које се користе са стандардним корисницима, а које се испоручују уз систем. Многи администратори се не сете да промене ове предодређене налоге.
  2. Покушати са свим кратким шифрама (са оним од једног до три карактера).
  3. Покушати са речима из online речника система или са листе вероватних шифара. Примери овог другог су доступни на "огласним таблама" (bulletin boards) хакера.

Технике упада (4)

4. Сакупити податке о корисницима, као што су њихова пуна имена, имена њихових супружника и њихове деце, слике из њихових канцеларија и књиге из њихових канцеларија које су повезане са њиховим хобијима.
5. Покушати са телефонским бројевима корисника, њиховим бројевима личне карте, пасоша, адресе, датума рођења.
6. Покушати са свим легитимним бројевима регистрације аутомобила из те државе.
7. Користити "тројанског коња" (Trojan horse) да се премосте забране приликом приступа.
8. Прислушкивати линију између удаљених корисника и система домаћина (host system).

Технике упада (5)

- Првих шест метода су различити начини за погађање шифре.
- Ако улъез мора да покуша да се улогује на систем, за сваки покушај погађања шифре, онда је то лако заустављив напад.
- Систем може једноставно да одбије било које логовање, након три покушаја са истог рачунара. Тако да би нападач морао да поново успоставља везу са системом.
- Под таквим околностима непрактично је испробавати велики број шифара.

Технике упада (6)

- Нападач тешко да ће покушати тако груб приступ.
- Већа је вероватноћа да ће, уколико на пример систем допушта приступ фајлу са шифрама и са малим нивоом привилегија, покупити тај фајл и трудити се да дешифрује неку шифру, колико год му за то буде потребно времена.
- Циљ му је да дође до шифре са већим привилегијама

Технике упада (7)

- Напади погађањем су изводљиви и веома ефикасни у случају када улъез може да испробава покушаје аутоматски и недетектован од стране система.
- Седми наведен начин упада са тројанским коњем може бити јако тежак за спречавање.
- На пример, корисник са ниским нивоом привилегија направио је игру и позвао је администратора система да је игра у слободно време.

Технике упада (7)

- Програм заиста и јесте био игра, али је у позадини извршавао код који копира фајл са шифрама у неки фајл овог корисника.
- Пошто фајл није био шифрован, већ само заштићен контролом приступа, администратор је играјући игру на свом налогу са правом приступа фајлу, омогућио улъезу да дође до фајла са шифрама.
- Осми приступ, прислушкивање линија, је проблем сигурности преноса података и може се спречити енкрипцијом.