Тема бр.11 Натрапници (Intruders)

11.1 Наведете ги и накратко дефинирајте три класи на натрапници.

Masquerader: Поединец кој не е овластен да го користи компјутерот и кој продира во системот за контрола на пристап за експлоатација на легитимна корисничка сметка.
Mispeasor: Легитимен корисник кој пристапува до податоци, програми или ресурси за кои таквиот пристап не е овластен или кој е овластен за таков пристап, но ги злоупотребува своите привилегии.
Скриен корисник (Clandestine user): Поединец кој се здобива со надзорна контрола врз системот и ја користи оваа контрола за да ги избегне контролите со ревизија и пристап или за сузбивање на собирање на ревизија.

11.2 Кои се двете општи техники за обезбедување на датотека со лозинки?

Еднонасочно (one way) криптирање: Системот чува само шифрирана форма на лозинката на корисникот. Кога корисникот ќе претстави лозинка, системот ја шифрира таа лозинка и ја споредува со зачуваната вредност. Во пракса, системот обично изведува еднонасочна трансформација (нереверзибилна) во која се користи лозинката за генерирање на клуч за функцијата за криптирање и во која се произведува излез со фиксна должина.
Контрола на пристап: Пристапот до датотеката со лозинки е ограничен на една или многу малку сметки.

11.3 Кои се трите предности кои што може да бидат дадени со систем за детекција на упади (IDS)?

1. Ако упадот е откриен доволно брзо, натрапникот може да биде идентификуван и исфрлен од системот пред да се направи каква било штета или некои од податоците да бидат компромитирани. Дури и ако откривањето не е доволно навремено брзо за да го идентификува натрапникот, колку побрзо ќе се открие упадот, толку е помала штетата и побрзо може да се постигне закрепнување.
2. Ефективен систем за откривање на упад може да послужи како пречка за напаѓачот, така дејствувајќи за спречување на упади.
3. Откривањето на упади овозможува собирање на информации за упадни техники што можат да се искористат за зајакнување на превенцијата на упад.

11.4 Која е разликата помеѓу статистичкото откривање на аномалија и откривање на упад врз основа на правило?

Статистичкото откривање на аномалија вклучува собирање податоци што се однесуваат на однесувањето на легитимните корисници во текот на еден временски период. Потоа, се применуваат статистички тестови на набљудуваното однесување за да се утврди со високо ниво на доверба дали тоа однесување не е легитимно однесување на корисник.

Откривањето врз основа на правило вклучува обид да се дефинира збир на правила што можат да се користат за да се одлучи дека даденото однесување е всушност однесување на натрапник.

11.5 Кои метрики се корисни за откривање на упад врз основа на профил?

- Бројач: Ненегативен цел број кој може да биде зголемен, но не намалена се додека не се ресетира со управувачка акција. Обично, број на одредени типови настани се чуваат за одреден временски период.
- Мерач (Gauge): Ненегативен цел број што може да се зголеми или намали. Обично, мерач се користи за мерење на тековната вредност на некој ентитет.
- Тајмер на интервали: Колку време поминало помеѓу два поврзани настани.
- Користење на ресурси: Количина на потрошени ресурси за време на одреден период.

11.6 Која е разликата помеѓу откривање на аномалија засновано на правило и идентификација на навлегување заснована врз правилата?

Со откривање на аномалија засновано на правило, историските записи за ревизија (audit) се анализирани за да ги идентификуваат шемите на употреба и автоматски да генерираат правила што ги опишуваат тие шеми. Правилата може да претставуваат однесување од минатоти корисници, програми, привилегии, временски слотови, терминали итн. Потоа, се набљудува сегашното однесување, и секоја трансакција се проверува дали одговара на множеството правила за да се утврди дали е во согласност со некое од историски набудуваните шеми на однесување.

Идентификацијата на навлегување заснована врз правилата користи правила за идентификување на познати навлегувања или навлегувања кои би ги искористиле познатите слабости. Исто така, може да бидат дефинирани правила кои идентификуваат сомнително однесување, дури и кога однесувањето е во границите на воспоставените модели на употреба. Обично, правилата кои се користат во овие системи се специфични за машината и оперативниот систем. Исто така, ваквите правила се генерираат од „експерти“, а не од средства за автоматска анализа на ревизорските записи.

11.7 Што е honeypot?

Honeypots се системи за што се дизајнирани да го намамат потенцијалниот напаѓач далеку од критичните системи. Тие се дизајнирани да:

- го пренасочат напаѓачот од пристап до критичните системи
- собираат информации за активноста на напаѓачот
- го охрабруваат напаѓачот да остане на системот доволно долго за администраторите да му одговорат

Овие системи се исполнети со лажни информации дизајнирани да изгледаат вредно, но легитимен корисник на системот нема да има пристап. Така, секаков пристап до информациите е осомничен. Системот е инструментиран со чувствителни монитори и логирачи на настани што ги детектираат овие пристапи и собираат информации за активностите на напаѓачот. Бидејќи било каков напад против honeypot е направен да изгледа успешно, администраторите имаат време да се мобилизираат и да го следат напаѓачот без воопшто да ги изложуваат продуктивните системи.

11.9 Наведете и накратко дефинирајте четири техники што се користат за да се избегнат лозинки кои лесно се погодуваат.

- Едукација на корисници: На корисниците може да им се објасни важноста за употреба на “тешки” лозинки и може да бидат обезбедени со упатства за избор на силни лозинки.
- Лозинки генерирани од компјутер: На корисниците им се обезбедени лозинки генерирани од компјутерски алгоритам.
- Реактивно проверување на лозинка: системот периодично извршува свој разбивач на лозинки за да пронајде лозинки кои лесно се погодуваат. Системот ги откажува било кои такви лозинки и го известува корисникот.
- Проактивна проверка на лозинка: на корисникот му е дозволено да избере своја лозинка. Меѓутоа, во моментот на селекција, системот проверува да види дали лозинката е дозволена и, ако не е, ја отфрла.