НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

## МАГИСТЪРСКИ ФАКУЛТЕТ

# ДЕПАРТАМЕНТ "ИНФОРМАТИКА"

**ПРОГРАМА „Софтуерни технологии в Интернет”**



### ЗАДАЧА ЗА ТЕКУЩА ОЦЕНКА

**КУРС: INFM102 Компютърна сигурност в Интернет**

**ТЕМА: Въпроси по задача 2**

**НА СТУДЕНТА** : Георги Иванов Георгиев

**Фак. №:** f88683

**Дата:** 06/01/2018 г.

**Преподавател:**

/ доц. В.Къдрев / …………………

София

**ВЪПРОС 1**

* 1. ***До какво води отвличането на сесия (Session Hijacking).***

Отговор: Отвличане на сесия представлява, пресичане на вече осъществена връзка (обикновено TCP) между две машини. Целта е да се получи достъп до сесия, в която се намират двете машини и да се отклони комуникацията през атакуващата машина. Тази техника пропуска автентикацията, тъй като се закача в комуникацията след като тя е била осъществена. Съществуват два вида отвличане:

* Активно – отвличане на сесия с цел да се пробие защита на машините
* Пасивно – подслушване на комуникацията между машини

Важно е да се отбележи, че има съществена разлика между отвличане и повтаряне на сесия. Повтарянето на сесия подправя уловените пакети и ги препраща към мишената. Отвличането на сесия подправя адреса на хакера, така че да съвпадне с инициализатора на сесията. Често това е част от DoS атака, за да може инициализатора на връзката да се измести от връзката. Отвличането бива:

* Открито преправяне – когато хакера придобива няколко пакета от комуникацията, взимайки от тях поредните и потвърждаващите номера на TCP сесията
* Сляпо преправяне – хакерът трябва да се намира на същия LAN и се опитва да отгатне поредните и потвърждаващите номера на TCP сесията
  1. ***До какво води атаката на услугата DNS.***

Отговор: Атаките се насочват към основната система осигуряваща работата на проткола TCP/IP. DNS се използва за транслиране на домейн имена в IP адреси.

Основни атаки насочени към DNS:

* DNS spoofing – подмяна на IP-тата към определени домейн имена
* Препълване на буфера – подмяна на домейн името с такова с твърде голяма дължина. Става чрез проваляне на проверката за дължина на името и препълване на буфера, чрез изпращане на по-голямо от 4 байта поле за дължина на име.
  1. ***По какво се различават методите за защита от злонамерен достъп - черен списък (blacklist) и бял списък (whitelist).***

Отговор: Черният списък представлява непрекъснато обновяем списък, в който всички обекти се определят като зловредни и тяхното изпълнение не се осъществява. Този метод е популярен сред антивирусните програми. Негови силни страни са ефективност в разпознаването на зловреден обект, за който вече съществува информация. Слаби страни са факта, че метода е реактивен а не проактивен – списък следва да се обновява навреме и не предпазва от първоначални заплахи. Също така той е доста ресурсоемък за машината, която го изпълнява.

Белият списък е пълна противоположност на черния. Той съдържа обекти, чието изпълнение е позволено, а на всичко извън него е забранено. Сили страни са че не изисква много ресурс за да се изпълнява (ако е конфигуриран правилно) и поставя доста високо ниво на защита. Слаби страни са изискването за непрекъснато обновяване и поддръжка в следствие на разширяване на системата.

* 1. ***По какво се различават класически HIPS (Host Intrusion Prevention System) и базирани на политика HIPS програми.***

Отговор: HIPS програмата има пълен контрол над функционирането на ОС система. Класическите HIPS предоставят много високо ниво на защита, по-малко ресурсоемки са от традиционната антивирусна програма и осигуряват контрол над зловредни обекти и над различни приложения работещи на машината. За целта потребителят трябва да е запознат с оперирането на съответната ОС. Важно условие е HIP да се инсталира на не заразена среда. Програмите базирани на HIPS политики функционират малко по-различно – те разделят приложенията на доверени и недоверени, като осигуряват различни нива на достъп до системните ресурси в зависимост от категорията. Приложения, които оперират с интернет ресурси се определят за недоверени и на тях не се разрешава достъп до системни обекти. Силните и слабите страни са идентични с тези на традиционните HIPs, но тук не се изискват много познания свързани с ОС.

* 1. ***Какво е мрежова устойчивост и какво е програмна устойчивост.***

Отговор: Мрежовата и програмната устойчивост спомагат защитата от атаки.

* Мрежова устойчивост – свързана е със мрежовите устройства, като ключова роля играе защитната стена като допълнение към router. Контролът на достъп на външни IP адреси сериозно намалява предпоставките за DoS атаки
* Програмната устойчивост – свързва се с програмите и най-общо с операционните системи. Тук съществува един неопределен фактор – програмният код се пише от хора и това често може да доведе до грешки. Необходимо е периодично обновяване на софтуера до последната възможна версия, за да се намалят пропуските в сигурността.

**ВЪПРОС 2**

***2.1. В какви случаи за защита от злонамерен достъп се използват евристики (heuristics) и блокатор на поведение (behaviour blocker).***

Отговор:

И двете техники търсят нередности в системата, като предприемат различни действия при локализирането им.

* Евристиките – вдигат аларма
* Блокаторите – преустановяват действието на дадения обект

***2.2.*** ***Как виртуализацията (virtualization) се използва за защита от злонамерен достъп.***

Отговор: Виртуализацията позволява изпълнение на приложения в контролирана среда. Приложенията не оперират директно с ресурсите на ОС, а преминават през виртуализиращ софтуер. По този начин може умишлено да се изпълняват заразени приложения, с цел да се наблюдава действието на антивирусния софтуер и да се отстраняват нередностите от него. При използването на виртуализация се консумират сравнително малко системни ресурси и изисква по-малко умения в сравнение с HIPs.

***2.3. Как конкретно защитната стена (Firewall) се използва за защита от злонамерен достъп.***

Отговор: Защитната стена предпазва от злонамерен достъп, като налага филтър на мрежовия трафик и по този начин следи, кой процес има достъп до интернет. Характеризира се с ниска ресурсоемкост. Трябва да се вземе предвид фактът, че защитната стена не осигурява пълна защита и винаги се използва в комбинация с цялостната архитектура за сигурност.

***2.4. Какви са основните архитектури на защитните стени.***

Отговор:

* Пакетно филтриращи – намират се в мрежовия слой на OSI, където се приема или отхвърля пакета на базата на предефинирани правила
* Кръгови – търсят валиден TCP handshake в сесията и ако няма такъв, я разпадат
* Прокси-сървърни – стената представлява прокси между клиента и сървъра и филтрира сигурните от несигурните мрежи
* Динамично пакетно филтриращи – разширение на филтриращата архитектура, чрез вземане на филтриращи решения, на база на данните в пакета и kernel proxy, работещ в основата на ОС

**ВЪПРОС 3**

***3.1. Каква е разликата между различните категории на firewall технологиите.***

Отговор: Основната разлика е различното ниво на защита.

Firewall работещи на базата на филтриране на пакети, изследват мрежово ниво, члез филтри на IP, тип на протокол, номер на порт на получател и подател, посока на трафика и интерфейса, на който е получен даден пакет. Биват stateless – не запомнят сесията между хостовете и statefull – запазват сесията. Това са защитните стени с най-ниска степен на защита поради факта, че не разбират от контекста на дадена връзка.

Защитните стени работещи на приложния слой от OSI контролират пакетите, които се изпращат между две мрежи. Те водят отчетност за всички осъществени връзки. Технологията се реализира чрез системи за алармиране, контролиране на достъпа и автентикация. Недостатък е факта, че всяко приложение има нужда от собствен gateway, както и че пакетите се анализират в приложния слой.

Multilayer Firewall позволяват филтриране на трафика във вътрешната мрежа.

***3.2. На кой слой от OSI модела се използва защитната стена.***

Отговор: Работата се извършва на един или повече слоеве. Най-често се поставя в мрежовия слой, като така се контролират всички пакети, които минават през нея. Тя може да работи и в приложния, сесийния и транспортния слой.

***3.3. Какво е демилитаризирана зона (DMZ).***

Отговор: DMZ е зоната между два firewall-а, където оперира потребителското приложение. Самите потребители са извън втората защитна стена и нямат директен достъп до приложението. Системите за следене на неоторизиран достъп работят с DMZ.

***3.4. Дайте примери за защита на физическия, каналния и мрежовия слой.***

Отговор:

* Физически слой – защитава се посредством ограничаване на достъпа до физическите устройства. Пример: ограничаване на достъпа до сървърното помещение, чрез въвеждане на система за оторизиране, премахване на конзолен достъп до устройствата от неоторизирани лица.
* Канален слой – конфигуриране на даден порт като access port (борба с прескачане на VLAN); ограничаване на броя и специфициране на MAC адресите, които се допускат до даден порт (борба с запълването на MAC таблицата); дефиниране на потребители и рутери (борба с ARP атаки); спиране на VTP протокола (борба с VTP атаки)
* Мрежов слой – най-сложният от трите. Пример е метода на конфигурацията на устройствата – забранява използването на несигурните Telnet и HTTP за конфигуриране и защита от инжектиране на зловредни маршрути, чрез избягване използването на RIP v1 поради липсата на автентикация.

***3.5. Дайте примери за защита на слоеве от транспортния до приложния.***

Отговор: Всички слоеве от транспортния до приложния са изложени на абсолютно всички видове атаки изложени по-горе, следователно и защитите приложими към по-долните важат и тук.

**ВЪПРОС 4**

***4.1. Какви са основните механизми за защита от DoS атаки.***

Отговор: Най-добрият начин за защита от DoS атаки е ако се подхожда внимателно и предпазливо когато изграждаме мрежата. Добри практики са да се поддържа последен софтуер и последните обновления на приложенията от трети страни, които ползва нашата система; да се изгражда и активно да се използва система следяща за неоторизиран достъп; да оборудваме системата с антивирусен софтуер. Важно е да се знае, че дори всички тези стъпки да са изпълнени отлично DoS атаката остава съвсем реална и опасна.

***4.2. Какви други механизми се използват за защита от DoS атаки.***

Отговор:

* Филтри на IP адреси известни с извършването на DoS атаки
* Правилно избиране на ресурсите на системата – ограничаване на отворените връзки, тяхното прекратяване или подмяна с новопостъпили

***4.3. Как за защита се използва Proxy технологията.***

Отговор: Тази технология се ограничава до LAN и малки WAN мрежи и представлява сървър, който приема целия мрежови трафик. В сървъра се извършват проверки свързани със сигурността, блокиране на входящ и изходящ трафик спрямо филтри. Плюс на технологията е кеширането на често посещавани страници.

***4.4. Какви са механизмите за защита на електронната поща.***

Отговор: Основно биват защити срещу СПАМ:

* филтри по ключови думи, html тагове, regex (регулярни изрази);
* техники за статистически анализ;
* филтър на специфични URL-и в съдържанието на имейла.
* Black list на адреси от които не се допускат съобщения или white list

***4.5. Какви са елементите на системите за откриване на нарушители (IDS).***

Отговор: IDS служат за автоматизиране на процеса на следене и анализ на сигурността на компютърните системи и мрежи. Използват се поради бързото алармиране за извършвана атака, като така осигуряват време и възможност за вземане на мерки за нейното блокиране. Най-общо имат 4 основни компонента:

* Детектори – събират информация и я изпращат към анализаторите
* Анализатори – бази данни, които биват мрежови или сървърни
* Модул за реакция и управление

***4.6. Какви са разликите между различните видове управление на IDS системи.***

Отговор:

* Централизирано управление – има една основна точка, която извършва следенето, анализа и обработката на информацията от него. Недостатък е, че ядрото представлява единствена точка на провал и ако то се засегне цялата IDS прекратява работата си.
* Частично разпределено управление – мениджмънта се разпределя между няколко локални възела в определена йерархия, които се управляват от един централен възел. При този вариант всеки локален възел се справя сам с откритата от него атака. Недостатък и тук е, че когато даден високопоставен възел преустанови работа всичко под него престава да работи.
* Разпределено управление – работят чрез самостоятелно функциониращи агенти в различни части на системата. Лесно се преконфигурират и добавят нови.
* Мрежово ориентирани системи – грижат се за откриване на нарушителите като следят мрежовите пакети. Те са най-популярни.

**ДИСКУСИЯ**

Какви са причините за различното разположение на сензорите на системите за откриване на нарушители.

Отговор: Основната причина се определя в зависимост от целите на администраторите на системата. Ако те искат да анализират поведението на служители или да се спазват стриктно политиките за сигурност те биха сложили сензорите в главните комуникационни възли на системата. Ако пък целта е да се види цялостната защита на системата макар и с риск от натоварване на самата IDS система сензорите биха били поставени пред или след външните защитни стени. Зад външната стена ще бъдат открити кои атаки не е успяла да спре и проблеми в нейната конфигурация. Пред външната стена ще се разберат вида и източниците на заплахите за тяхната система. Също така би могло сензорите да се поставят в критичните модули на системата.