Міністерство освіти і науки України Донбаська державна машинобудівна академія

МЕТОДИЧНІ ВКАЗІВКИ

до лабораторних робіт

з дисципліни

«АДМІНІСТРУВАННЯ КОМП'ЮТЕРНИХ МЕРЕЖ»

(для студентів спеціальності 123"Комп'ютерна

інженерія»)

Освітній рівень - бакалавр

Краматорськ 2020

ЛАБОРАТОРНА РОБОТА № 1. УСТАНОВКА І КОНФІГУРАЦІЯ ОПЕРАЦІЙНОЇ СИСТЕМИ НА ВІРТУАЛЬНУ МАШИНУ

1.1. Мета роботи

Метою даної роботи є набуття практичних навичок установки операційної системи на віртуальну машину, настройки мінімально необхідмих для подальшої роботи сервісів.

1.2. Вказівки до роботи

1.2.1. Технічне забезпечення

Лабораторна робота має на увазі установку на віртуальну машину VirtualBox (https://www.virtualbox.org/) операційної системи Linux (дистрибутив CentOS).

Вимоги до технічного і програмного забезпечення:

- Intel Core i3-550 3.2 GHz, 4 GB оперативної пам'яті, 8 GB вільного місця на жорсткому диску або вище;

- OC Linux Gentoo

- VirtualBox верс. 4.3.18 або старше.

1.2.2. Угоди про іменування

При виконанні робіт слід дотримуватися наступних правил іменування: - користувач всередині віртуальної машини повинен мати ім'я, що збігається з логіном студента, що виконує лабораторну роботу. Ви можете подивитися використовувати ваші дані, набравши в терміналі команду:

id -un

- ім'я хоста вашої віртуальної машини повинно співпадати з логіном студента, виконує лабораторну роботу.

- ім'я віртуальної машини повинно співпадати з логіном студента, що виконує лабораторну роботу.

1.3. Послідовність виконання роботи

Завантажте в дисплейному класі операційну систему Linux. Здійсніть вхід в систему.Запустіть термінал. Перейдіть в каталог / Var / tmp:

cd/ Var / tmp

Створіть каталог з ім'ям користувача (що співпадає з логіном студента в дисплейном класі). Для цього можна використовувати команду:

```
mkdir / var / tmp /`id -un`
```

Запустіть віртуальну машину, ввівши в командному рядку: VirtualBox & перевірте у властивостях VirtualBox місце розташування каталогу для віртуальних машин. Для цього в VirtualBox виберіть **Файл-Свойства**, вкладка загальні.

В полі Папка для машин (Рис. 1.1) має стояти / Var / tmp / имя_пользователя, де Ім'я користувача- логін (обліковий запис) студента в групі. Якщо зазначений інший каталог, то потрібно змінити його, Як зазначено вище.

🎸 Virt	tualBox - Настро	ойки		~ ^ X
	Общие	Общие		
	Ввод	Папка <mark>для <u>м</u>ашин по умолчанию:</mark>	/var/tmp/user T	*
S	Обновления	<u>Б</u> иблиотека аутентификации VRDP:	VRDPAuth	•
	Язык			
	Дисплей			
	Сеть			
	Плагины			
	прокси			
			От <u>м</u> ена	<u>о</u> к

Рис. 1.1. Вікно «Властивості» VirtualBox

Створіть нову віртуальну машину. Для цього в VirtualBox виберіть Машина-Створити .Вкажіть ім'я віртуальної машини (ваш логін в групі), тип операційної системи - Linux, RedHat (рис. 1.2).

🖉 создать виртуальную м	ашину					^ X
	Укажи	те имя и тип ОС				
~~~~	Пожалуі операци машину данной	йста введите имя новой ви 1онной системы, которую В . Заданное Вами имя будет машины.	ртуальной машин Вы собираетесь ус использоваться	чы и выберите тановить на д для идентифик	тип анную ации	
	<u>И</u> мя:	user			- 24	
	<u>т</u> ип:	Linux			-	
	<u>В</u> ерсия:	Red Hat (64-bit)			•	_
		<u>Э</u> кспертный режим	< <u>Н</u> азад	Далее 📐	Отмена	a

## Рис. 1.2. Вікно «Ім'я машини і тип ОС»

Вкажіть розмір основної пам'яті віртуальної машини - 1024 МБ (рис. 1.3).

💱 Создать виртуальную м	ашину				• :•	×
~~~	Укажите объём п Укажите объём оператив виртуальной машине. Рекомендуемый объём р	<b>амяти</b> ной памяти (RAM) выделенн авен <b>1024</b> МБ.	ый данно	рй		
	4 МБ	n (1616), (1600), (16	8192 M5	1024	Ţ	МБ
		< <u>Н</u> азад Вг	теред >	Отм	ена	

Рис. 1.3. Вікно «Розмір основної пам'яті»

Задайте конфігурацію жорсткого диска - завантажувальний, VDI (BirtualBox Disk Image), динамічний віртуальний диск (рис. 1.4-1.6).

🎲 Создать виртуальную 🛚	ашину ~ ~ ~
	Жесткий диск
,	При желании к новой виртуальной машине мо ${\mathbb Y}$ но подключить виртуальный жёсткий диск. Вы можете создать новый или выбрать из уже имеющихся.
	Если Вам необходима более сложная конфигурация Вы можете пропустить этот шаг и внести изменения в настройки машины после её создания.
	Рекомендуемый объём нового виртуального жёсткого диска равен 8,00 ГБ.
	<u>Н</u> е подключать виртуальный жёсткий диск
	Осоздать новый виртуальный жёсткий диск
	Использовать существующий виртуальный жёсткий диск
	🛕 Base.vdi (Обычный, Недоступен) – 🗔
	< Назад Создать Отмена

Рис. 1.4. Вікно підключення або створення жорсткого диска на віртуальній машині

💱 Создать виртуальный	і жёсткий диск	- · · ×
	Укажите тип	
	Пожалуйста, укажите тип файла, определяющий формат, который Вы хоти создании нового жёсткого диска. Если у Вас нет необходимости использо продуктами программной виртуализации, Вы можете оставить данный па	ите использовать при вать диск с другими араметр без изменений.
	VDI (VirtualBox Disk Image)	
	O VHD (Virtual Hard Disk)	
	O VMDK (Virtual Machine Disk)	×
	Экспертный режим	Вперед > Отмена

Рис. 1.5. Вікно визначення типу підключення віртуального жорсткого диска



Мал. 1.6. Вікно визначення формату віртуального жорсткого диска Задайте розмір диска - 40 ГБ (або більше), його розташування - в даному випадку /var/tmp/iмя пользователя/centos.vdi(Puc. 1.7).

Виберіть в VirtualBox Свойства Носители вашій віртуальній машини. Додайте новий привід оптичних дисків і виберіть образ /afs/dk.sci.pfu.edu.ru/common/files/iso/CentOS-7-x86_64-DVD.iso (Рис. 1.8).



Рис. 1.7. Вікно визначення розміру віртуального динамічного жорсткого диска і його розташування



Рис. 1.8. Вікно «**Носители**» віртуальної машини: вибір способу оптичного диска

Запустіть віртуальну машину, виберіть мову інтерфейсу і перейдіть до налаштування установки операційної системи (рис. 1.9).

При необхідності скорегуйте часовий пояс, розкладку клавіатури (рекомендуется як мову за замовчуванням вказати англійську мову).



Рис. 1.9. Вікно настройки установки образу ОС

У розділі вибору програм вкажіть в якості базового оточення Сервер с GUI, а як доповнення – Средства разработки (Рис. 1.10).

Вимкніть KDUMP (рис. 1.11).

Місце установки ОС залиште без зміни (рис. 1.12).

Увімкніть мережеве з'єднання і в якості імені вузла вкажіть імя_пользователя.localdomain(Рис. 1.13).

Встановіть пароль для root і користувача з правами адміністратора (Рис. 1.14-1.16).

Після завершення установки операційної системи коректно перезапустите віртуальну машину і прийміть умови ліцензії (рис. 1.17-1.18).

У VirtualBox оптичний диск повинен відключитися автоматично, але якщо це не відбулося, то необхідно відключити носій інформації з образом, вибравши Свойства Носители CentOS-7-х86_64-DVD.iso Удалить устройство.

	VCTAHOBKA CENTOS LINU EB us
вовое окружение	Дополнения для выбранного окружения
Монискительна установка Валаза функциональность. Сопри се Node Установка для соплителния соникцистики и общействи. Сопри се при для соплителния соникцистики и общействи. Спри се уморактируютури Сприкер нарактируютури Саркер кралистики физика и основни для предлаговой. Спри се уморактируютури. Саркер нарактири сели сели сели для предлаговой. Спри се уморактируютури. Саркер нарактируютури. Саркер нарактири сели сели сели для предлаговой. Спракер рабо сели сели сели сели предлаговой. Спракер рабо периостики сели сели сели сели на для неконоското Интерностивности. Хосе кортуровозация Маниева сели сели сели сели сели сели сели сели	Средства возпроизе производите выпости: Средства возпроизе производите выпости: Средства диализат производите выпости: Средства диализати састении и производительности на уражне произволяся. Сераке Ренетра SQL SQL - сераке Ленета SQL SQL - сераке Ленета (Дунецисантровать и сенества серакра венати Силанизат састение функцисантровать и сенества серакра венати Тизализат састение функцисантровать и сенества серакра венати Хакента састение функцисантровать и сенества серакра венати Удерство уражителисти упределения Сель OS Linux, заключее OpenLMI с SIMPP Надения производительности и производительноства на управление серакра венати Кинента срад установани и производительно кнутуразовации. Рекерство сенествание управление застенае внутурательнае Средство производие уражение Библеотески сенества Селеб У Ципи, заключее образани. Библеотески сенествании управление внутурательные образани. Библеотески сенественства браноство сенества седакрания с средства ракователение уракование внутурательные образани. Библеотески сенественства браноство сенествания с сенества на опускатории уракование внутурательные образани. Библеотески сенественства браноство сенествание серакрание с сенества на опускаторие уракование с серакрание с селества ракователение уракование собразания. Библеотески сенествание с селествание с селества ракование селествание с селествание с образания. Селества ракование селествание с селествание с селества ракование селествание с селествание с селествание с селества ракование селествание с селествание с селества ракование селествание с селества ракование селествание с селества ракование селествание с селества ракование с селества ракование селествание с селества ракование селествани с селества рак

Рис. 1.10. Вікно настройки установки: вибір програм



Рис. 1.11. Вікно настройки установки: відключення КDUMP

an tes Malanami (Kada Mil Amadasa)	
Calif. Millions Bag Blag StreekTas Clearawa	
место установки	yctahoska centos unux 7 El m Cryses
набар устройсти Вибергите истройсти для установки отвродинный бистена. Они не установки в ставика колон. Личение и колон.	е будут изменени, до тео теор, пока вы их изменете нистку «Начать
AT A VECK HARDDYSK STA VECK HARDDYSK SSI / 8192 Mid costozio	
Decumentapositese: e consec gente	Processo a gray i tatani anĝonero gra anto
рууны паранетурь хранного данных Разбольно — Спольствать источеточного () Польтрого радения	attensionen angen opringen med over an and an ender
 Representation of the second se	

Рис. 1.12. Вікно настройки установки: місце установки



Рис. 1.13. Вікно настройки установки: мережа і ім'я вузла



Рис. 1.14. Вікно конфігурації користувачів

🧱 centos (Paliotaer) - Cracle VM Virtualbox		the second s	Conception in the
Файл Машина Вид Ввод Устройства Справка			
ПАРОЛЬ ROOT		УСТАНОВКА С	ENTOS LINUX 7
The Property of the Property o		El us	Спранка
Учетная запись админис Пароль root:	пратора (root) предназначена для управления сист	еной. Введите паропы поот.	
Подтверждание		Простой	
		20#205#0	

Рис. 1.15. Установка пароля для root

Файл Машина Вид Веод Устройства Справка		_
СОЗДАНИЕ ПОЛЬЗОВАТЕЛЯ	YCTAHOBKA CENTOS LINUX	7
(Trans	🖽 us Chipaesa	
Полное има	user	
Ина пользователя	user	
	Подсказка. Имя пользователя можит содержать до 32 знаков без пробетов.	
	🗹 Сделить этого полькователя администратором	
	Требнаать паропыдря мляй учетной запаков	
Пароль		
	Apocroè	
Подтвердите пароль	······ •	
	Дополнительно	
	🙆 🖸 🖉 🖉 💷 🗮 🕼 🍃 🗊 Приный С	tri.

Рис. 1.16. Установка пароля для користувача з правами адміністратора

Файл Машина Ви	ввод Устройства Справка	
-	ПЕРВАЯ НАСТРОЙКА	CENTOS LINUX 7 (CORE)
CentOS	LICENSING	
	СИСТЕМА Пицензия не ориената	
	сеть и имя узла Проводное соединенenpQs3) установлено	
	Baractus	Tempurre
	Од Запалнате стилиение секции, прежда чем терейти к сперунцему шату.	
		🖬 🕞 🥐 🖉 🗮 🗮 🔛 🥥 🕑 Праный Ctrl

Рис. 1.17. Первісна настройка ОС



Рис. 1.18. Первісна настройка ОС: ліцензія

Увійдіть до системи з заданою вами при установці обліковим записом. В меню Устройства віртуальної машини підключіть образ диска доповнень гостьовий ОС (Рис. 1.19), при необхідності введіть пароль користувача гоотвашої віртуальної ОС.



Мал. 1.19. Підключення образу диска доповнень гостьовий ОС

Після завантаження доповнень натисніть Return або Enter (Рис. 1.20) і коректно перезавантажте віртуальну машину.



Рис. 1.20. Завершення підключення образу диска доповнень гостьовий ОС

1.3.1. Установка імені користувача і назви хоста

Якщо при установці віртуальної машини ви задали ім'я користувача або ім'я хоста, що не задовольняє угодою про іменування (див. розділ 1.2.2), то вам необхідно змінити це.

1. Запустіть віртуальну машину і залогініться.

2. Запуск термінал і отримаєте повноваження адміністратора: su -

3. Створіть користувача (замість usernameвкажіть ваш логін в групі):

adduser -G wheel username

4. Задайте пароль для користувача (замість username вкажіть ваш логін в групі):

passwd username

5. Встановіть ім'я хоста (замість usernameВкажіть ваш логін в групі):

6. Перевірте, що ім'я хоста встановлено вірно:

Hostnamectl

1.4. Домашнє завдання

Дочекайтеся завантаження графічного оточення і відкрийте термінал. У вікні терміналу проаналізуйте послідовність завантаження системи, виконавши команду

dmesg.

Можна просто переглянути висновок цієї команди:

dmesg | less

Можна використовувати пошук за допомогою grep:

dmesg | grep -i"Te, що шукаємо"

Отримайте наступну інформацію.

- 1. Версія ядра Linux (Linux version).
- 2. Частота процесора (Detected Mhz processor).
- 3. Модель процесора (СРИО).
- 4. Обсяг оперативної пам'яті (Memory available).
- 5. Тип виявленого гипервизора (Hypervisor detected).
- 6. Тип файлової системи кореневого розділу.
- 7. Послідовність монтування файлових систем.

1.5. зміст звіту

Звіт повинен включати:

1) титульний лист;

2) формулювання завдання роботи;

3) опис результатів виконання завдання:

- короткий опис дії;

- команду що вводиться або команди;
- результати виконання команд (знімок екрану);

4) висновки, узгоджені із завданням роботи;

5) відповіді на контрольні питання;

6) звіт про виконання додаткового завдання.

1.6. Контрольні питання

- 1. Яку інформацію містить обліковий запис користувача?
- 2. Вкажіть команди терміналу і наведіть приклади:
- для отримання довідки по команді;
- для переміщення по файлової системи;
- для перегляду вмісту каталогу;

- для визначення обсягу каталогу;

- для створення / видалення каталогів / файлів;

- для завдання певних прав на файл / каталог;

- для перегляду історії команд.

3. Що таке файлова система? Наведіть приклади з короткою характеристикою.

4. Як подивитися, які файлові системи подмонтіровать в ОС?

5. Як видалити завислий процес?

При відповідях на контрольні питання рекомендується ознайомитися з інформацією з [1-12].

Список літератури

1. *Купер М.* Мистецтво програмування на мові сценаріїв командної пролочки. - 2004. - URL:https: / / www. opennet. ru / docs / RUS / bash _scripting_guide /.

2. *Newham C.* Learning the bash Shell: Unix Shell Programming. - O'Reilly Media,2005. - 354 p. - (In a Nutshell). - ISBN 0596009658.

3. *Робачевскій А., Немнюгин С., Стесік О*.Операційна система UNIX. - 2-е изд. - БХВ-Петербург, 2010. - 656 с. - ISBN 978-5-94157-538-1.

4. Колісниченко Д. Н. Самовчитель системного адміністратора Linux. - СПб. :БХВ-Петербург, 2011. - 544 с. - (Системний адміністратор). - ISBN 978-5-9775-0639-7.

5. *Dash P.* Getting Started with Oracle VM VirtualBox. - Packt Publishing Ltd, 2013. - 86 p. - ISBN 1782177825.

6. Unix i Linux: керівництво системного адміністратора / Е. Немет, Г. Снайдер, Т. Р. Хейн, Б. Уейл. - 4-е изд. - Вільямс, 2014. - 1312 с. - ISBN 978-0-13-148005-6.

7. *Colvin H.* VirtualBox: An Ultimate Guide Book on Virtualization with Virtual-Box. - CreateSpace Independent Publishing Platform, 2015. - 70 p. – ISBN 978-1522769880.

8. *Таненбаум Е., Бос Х.* Сучасні операційні системи. - 4-е изд. - СПб. :Пітер, 2015. - 1120 с. - (Класика Computer Science).

9. GNU Bash Manual. - 2016. - URL:https: / / www. gnu. org / software /bash / manual /.

10. *Robbins A.* Bash Pocket Reference. - O'Reilly Media, 2016. - 156 p. - ISBN978-1491941591.

11. *Vugt S. van.* Red Hat RHCSA / RHCE 7 cert guide: Red Hat Enterprise Linux 7(EX200 and EX300). - Pearson IT Certification, 2016. - 1008 p. - (Certification Guide). - ISBN 978-0-7897-5405-9.

12. Zarrelli G. Mastering Bash. - Packt Publishing, 2017. - 502 p. - ISBN 9781784396879

ЛАБОРАТОРНА РОБОТА № 2 НАЛАШТУВАННЯ МІЖ МЕРЕЖЕВОГО ЕКРАНУ

Мета роботи: навчитися виконувати налаштування між мережевого екрану

Хід роботи

Налаштування міжмережевого екрану CentOS 6

1. Налаштувати дві віртуальні машини CentOS Linux та встановлено мережевий зв'язок між ними.

2. Перевірити зв'язок між двома віртуальними машинами за допомогою команди ping.

3. Перевірити поточні налаштування між мережевого екрану iptables, за допомогою команди:

iptables –L

4. Видалити стандартно встановлені правила за допомогою команди

iptables –F

і бачимо, що усі правила очищено.

5. Заборонити на першій віртуальній машині виконання команди ping, для чого за допомогою інтерфейсу керування роботою міжмережевого екрану, налаштувати правило в iptables на заборону передачі ICMP пакетів.

iptables -I INPUT -p icmp --icmp-type 8 –j DROP

6. Перевірити, що правило встановлено у ланцюгу iptables:

7. Перевіряємо правильність встановленого правила, за допомогою команди ping, що у результаті показує як пакети блокуються у заданому нами напрямку.

8. Перевірити чи залишились інші види доступу, наприклад через SSH.

9. Виконати налаштування прав міжмережевого екрану відповідно до заданого варіанту.

	Табл	иця 5.1
	Bap	Завдання
иант		
	1	 Заборонити/дозволити вхідний трафік конкретній ір-
		адресі. наприклад
		основна машина або інша віртуальна або навіть глобальна
		— заборонити вхідний трафік по протоколу Telnet
		(локально)

	— заборонити вихідний трафік по протоколу telnet до
	конкретної ір-адреси
2	Заборонити дозволити вихідний трафік до конкретної ір-
	адреси. наприклад
	основна машина або інша віртуальна або навіть глобальна
	- заборонити вихідний трафік по протоколу telnet
	- заборонити вхідний трафік по протоколу telnet
	конкретній ір-адресі
	(.локально)
3	- Заборонити дозволити вхідний ісіпр-трафік конкретній
	ір-адресі
	— заборонити вхідний трафік по протоколу ftp (локально)
	— заборонити вихідний трафік по протоколу ftp до
	конкретної ір-адреси
4	 Заборонити дозволити вихідний істр-трафік до
	конкретної ір-адреси
	- заборонити вихідний трафік по протоколу ftp
	— заборонити вхідний трафік по протоколу ftp конкретній
	ір-адресі
	(локально)
5	- Заборонити дозволити вхідний трафік з конкретної веб-
	адреси (доменного
	IMEHI)
	— заборонити вхідний трафік по протоколу smtp
	^{(л} локально)
	— заооронити вихідний трафік по протоколу smtp до
6	Сервера (веб абб пр-адреси)
0	заобронити дозволити вихідний трафік до конкретної вео-
	(доменного імені)
	- заборонити вихілний трафік по протоколу smtp
	- заобронити вхідний трафік по протоколу зпіцр конкретни
7	- Заборонити дозволити вхідний трафік з конкретної веб-
,	алреси (доменного
	імені)
	— заборонити вхілний трафік по протоколу рорЗ
	(локально)
	— заборонити вихідний трафік по протоколу рорЗдо
	конкретної адреси-
	сервера (веб або ір-адреси)

8	Заборонити дозволити вихідний трафік до конкретної вео-
	адреси
	(доменного імені)
	 заборонити вихідний трафік по протоколу рорЗ
	- заборонити вхідний трафік по протоколу рорЗ конкретній
	ір-адресі
	(локально)
9	 — Заборонити дозволити вхідний трафік з конкретної вео-
	адреси (доменного
	імені)
	— заборонити вхідний трафік по протоколу ііпар
	(локально)
	— заборонити вихідний трафік по протоколу ііпар до
	конкретної адреси-
	сервера (веб або ір-адреси)
10	Заборонити дозволити вихідний трафік до конкретної вео-
	адреси
	(доменного імені)
	- заборонити вихідний трафік по протоколу ііпар
	- заборонити вхідний трафік по протоколу ііпар конкретній
	ір-адресі
	(локально)

Частина 2. Налаштування мережевого екрану, скрипти АРF

1. Встановити APF. (APF – використовує фільтри на основі iptables, має більш розгалужену і гнучку систему налаштування) на віртуальну машину CentOS, використовуючи такі команди.

wget http://www.rfxn.com/downoads/apf-current.tar.gz tar -zxvf apf-current.tar.gz cd apf-9.7-1 sh ./install.sh

2. Налаштувати конфігураційний файл за допомогою команди :

vi /etc/apf/conf.apf

3. Для початку встановити мережевий інтерфейс.

DEVEL_MODE= може приймати значення 1 і 0. Значення 0 встановлює режим роботи APF у тестувальному режимі, тобто працює 5 хвилин і потім вимикається. Значення 1 – працює повноцінно.

4. Відредагувати файл

deny/allow_hosts.rules

Для того, щоб дозволяти/блокувати порти (TCP/UDP), прописати IP, які дозволяємо або блокуємо.

5. У файлі postroute.rules прописати правила пакетного фільтра, на основі iptables.

6. Для запуску APF виконати команду:

/usr/local/sbin/apf –(параметр).

В якості параметра можна використовувати :

-s - запуск -r - рестарт -f - стоп -l - статистика -st- статус

7. Скористатися командою

service apf (restart, start, stop).

8. Перевірити мережеві налаштування адаптера

vi /etc/sysconfig/network-scripts/ifcfg-eth0

9. Перезавантажити мережевий сервіс:

service network restart

10. Перезавантажити сервіс

apf: service apf restart

11. Переглядаємо правила iptables, які прописав сервіс apf, та записуємо ці правила у файл:

iptables –L > /rules_iptables.apf,

переглядаємо отриманий файл Виконати звіт з виконаних робіт, в тому числі показати скріншоти та

проаналізувати правила, які встановлює Apf

Частина 4 (опційна)

Дослідити програмне забезпечення, що виконує функції міжмережевих

екранів для мобільних платформ. Продемонструвати приклади їх застосування

ЛАБОРАТОРНА РОБОТА №3 ДОСЛІДЖЕННЯ ПРОТОКОЛУ SSL. НАЛАШТУВАННЯ ПІДТРИМКИ ЗАХИЩЕНИХ НТТР- З'ЄДНАНЬ (НТТРS)

Мета: дослідити особливості функціонування протоколу SSL та отримати практичні навички по створенню власних сертифікатів засобами OC сімейства Linux.

Хід роботи

Частина 1. Створення SSL-сертифікату для веб-серверу Nginx в OC CentOS.

1. Паредбачається, що ви уже маєте налаштовану віртуальну машину на основі CentOS із встановленим веб-сервером Nginx.

2. Створюємо каталог для збереження сертифікатів

mkdir /etc/nginx/ssl

3. Генеруємо в створений каталог файли сертифікату:

openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout /etc/nginx/ssl/nginx.key -out /etc/nginx/ssl/nginx.crt

У ході генерування будуть задані деякі запитання для встановлення службової інформації.

4. Додаємо до файлу конфігурації nginx ще одну секцію server такого виду:

```
server {
listen 80 default_server;
listen [::]:80 default_server;
listen 443 ssl;
root /usr/share/nginx/html;
index index.html index.htm;
server_name your_domain.com;
ssl_certificate /etc/nginx/ssl/nginx.crt;
ssl_certificate_key /etc/nginx/ssl/nginx.key;
location / {
try_files $uri $uri/ =404;
}
```

5. Перезапускаємо сервіс:

service nginx restart

6. Перевірка роботи сервера в захищеному режимі

Частина 2. Захоплення та аналіз пакетів в SSL сесії

Першим кроком є захоплення пакетів в SSL сесії. Щоб зробити це, ви повинні перейти на свій улюблений інтернет-магазин і почати процес покупки товару (але відмінити, перш ніж здійснити покупку!). Після захоплення пакетів Wireshark, ви повинні встановити фільтр так, щоб він відображав тільки кадри Ethernet, які містять записи SSL відправлені і отримані від хоста. (Запис типу SSL-це те ж саме, що і повідомлення SSL).

Якщо у вас є труднощі з перехопленням пакетів, ви можете завантажити apxiв http://gaia.cs.umass.edu/wireshark-labs/wireshark-traces.zip і розпакувати файл перехоплення пакетів *ssl-ethereal-trace-1*.

2. Огляд перехоплених файлів

Wireshark повинен відображати тільки Ethernet кадри, які мають SSL записи. Важливо мати на увазі, що кадр Ethernet може містити один або декілька записів SSL. (Це дуже відрізняється від HTTP, де кожен кадр містить або одне повне повідомлення HTTP або частину повідомлення HTTP.) Крім того, якщо SSL запис не може повністю вміститися в кадр Ethernet, то він буде пересланий у кількох кадрах. Дайте відповідь на наступні питання. Коли це можливо покажіть роздруківку пакета за допомогою якої Ви дали відповідь на питання. Підпишіть роздруківку, щоб пояснити свою відповідь. Щоб роздрукувати пакет використайте File->Print, оберіть Selected packet only, оберіть Packet summary *line*, і оберіть мінімальну кількість деталей пакету які потрібні Вам для відповіді. Хід виконання

1. Для кожного з перших 8 кадрів Ethernet, вказати джерело кадру (клієнта або сервера), визначити кількість записів SSL, які включені в кадрі, і список типів SSL записів, включених в кадрі. Намалюйте часову діаграму між клієнтом і сервером, з одного стрілкою для кожного запису SSL.

2. Кожен з SSL записів починається з трьох однакових полів (можливо, з різними значеннями). Один з цих полів "тип вмісту" і має довжину один байт. Перерахуйте всі три поля і їх довжини.

1.Розгорнути запис ClientHello. (Якщо ваше перехоплення містить кілька записів ClientHello, розкрити кадр, у якому міститься перший запис ClientHello.) Яке значення типу вмісту?

2.Чи містить запис ClientHello одноразове слово (також відоме як "виклик")? Якщо так, яке значення матиме "виклик" в шістнадцятковій системі числення?

3.Чи запис ClientHello називає які кібер-номери він підтримує? Якщо так, у першому з перерахованих номерів, якими є алгоритм з відкритим ключем, з симетричні ключем, і хешем?

4.Знайдіть запис SSL ServerHello. Чи вказує цей запис на обраний шифр? Які алгоритми використовуються в обраному шифру?

5.Чи має це запис одноразове слово? Якщо так, то якої довжини? Яке призначення клієнтських і серверних одноразових слів у SSL записі? 6. Чи містить цей запис ID сесії? Що є метою ID сесії? 7. Чи містить цей запис сертифікат, чи сертифікат включений в окремий запис. Чи можна вмістити сертифікат в один Ethernet кадр?

8.Знайдіть запис обміну клієнтськими ключами. Чи містить цей запис premaster secret? Для чого цей секрет використовується? Чи є секрет зашифрованим, якщо так, то яким чином? Яку довжину має зашифрований секрет?

9. Яка ціль запису Change Cipher Spec? Скільки байт у записі, що ви перехопили?

10. Що шифрується у зашифрованому записі-рукостисканні, і яким чином?

11. Чи сервер також відправляє запис зміни шифру і зашифрований запис- рукостискання для клієнта? Як ці записи відрізняються від тих, що відправлені клієнтом?

12. Як програмні дані шифрується? Чи записи, що містять дані програми включають MAC? Чи може Wireshark розрізнити зашифровані дані додатку і MAC?

13. Прокоментувати і пояснити все те, що ви знайшли цікавим у перехоплених даних.

Контрольні питання

1. Протокол SSL/TLS (VPN на транспортному рівні)

2. Протокол SSL/TLS. Архітектура

3. Протокол SSL/TLS. Change Cipher Spec Protocol

4. Протокол SSL/TLS. Alert Protocol

5. Протокол SSL/TLS. Handshake protocol

6. Протокол SSL/TLS. SSL Record Protocol

7. Протокол SSL/TLS. Ceciï

8. Протокол SSL/TLS. Переваги та недоліки____