

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ**

Кафедра інформаційних технологій та кібербезпеки факультету №4

**МЕТОДИЧНІ МАТЕРІАЛИ
ДО ЛАБОРАТОРНИХ ЗАНЯТЬ**

із навчальної дисципліни "Кібербезпека"
обов'язкових компонент
освітньої програми першого рівня вищої освіти

125 "Кібербезпека" (Протидія кіберзлочинності)

Харків 2020

ЗАТВЕРДЖЕНО

Науково-методичною радою
Харківського національного
університету внутрішніх справ
Протокол від 23.09.2020 № 9

СХВАЛЕНО

Вченою радою факультету №4
Протокол від 16.09.2020 № 5

ПОГОДЖЕНО

Секцією науково-методичної ради
ХНУВС з технічних дисциплін
Протокол від 18.09.2020 № 5

Розглянуто на засіданні кафедри інформаційних технологій та кібербезпеки (протокол від 15.09.2020 № 16)

Розробник: професор кафедри інформаційних технологій та кібербезпеки ХНУВС,
к.т.н. доцент Носов В.В.

Рецензенти:

доцент кафедри інформаційних технологій та кібербезпеки факультету №4 Харківського національного університету внутрішніх справ к.т.н. доцент Тулупов В.В.

завідувач кафедри інформаційних управляючих систем Харківського національного університету радіоелектроніки, д.т.н. професор Петров К.Е.

1. Розподіл часу навчальної дисципліни за темами

Номер та назва навчальної теми	Кількість годин відведених на вивчення навчальної дисципліни					Вид контролю
	Всього	з них:				
		лекцій	Практичні заняття	Лабораторні заняття	Самостійна робота	
Семестр №6						
Тема №1. Основні відомості про кібербезпеку	16	6	2		8	залік
Тема №2. Пасивний збір інформації	36	8	4	6	18	
Тема №3. Активний збір інформації про мережу	36	8	4	6	18	
Тема №4. Механізми захисту мережі від збору інформації, сканування та проникнення	32	8	4	6	16	
Тема №5. Застосування криптографічних сервісів	36	8	4	6	18	
Тема №6. Аналіз трафіку в комп'ютерних мережах	32	8	4	6	16	
Тема №7. Перехоплення сесій передачі даних в комп'ютерних мережах	36	8		6	18	
Тема №8. Безпека в безпроводних мережах	36	8	4	6	18	
Тема №9. Безпека в операційних системах	40	10	4	6	20	
Всього за семестр №6	300	72	30	48	150	
Семестр №7						
Тема №10. Шкідливе програмне забезпечення	24	6	4	4	12	екзамен
Тема №11. Переповнення буферу	24	6		4	12	
Тема №12. Безпека веб-серверів та веб-застосувань	32	6	6	6	16	
Тема №13. Атака «відмова в обслуговуванні»	24	6		4	12	
Тема №14. SQL-ін'єкції	32	6	4	6	16	
Тема №15. Соціальна інженерія	24	6	4	4	12	
Тема №16. Тестування на вразливість до атак	20	4		4	10	
Всього за семестр №7	180	40	18	32	90	
Всього за дисципліною	480	112	48	80	240	

2. Методичні вказівки до лабораторних занять

Тема №2. Пасивний збір інформації

Лабораторне заняття 1. Пасивний збір інформації

Навчальна мета заняття: навчитися користуватися програмними засобами пасивного збору інформації про об'єкт атаки при тестуванні безпеки

Кількість годин: 6 год.

Навчальні питання

1. Збір інформації про веб-сайти
2. Збір інформації за допомогою Google
3. Збір інформації за допомогою Whois
4. Збір інформації DNS

5. Збір інформації про мережу

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику пасивному збору інформації. Надати посилання до місця розміщення дистрибутивів програмних інструментів.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №3. Активний збір інформації про мережу

Лабораторне заняття 2. Активний збір інформації про мережу

Навчальна мета заняття: навчитися користуватися програмними засобами активного збору інформації про мережу при тестуванні безпеки

Кількість годин: 6 год.

Навчальні питання

1. Засоби для перевірки доступності вузла
2. Засоби для визначення ОС
3. Сканування портів
4. Перехоплення банерів

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику активному збору інформації. Надати посилання до місця розміщення дистрибутивів програмних інструментів.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №4. Механізми захисту мережі від збору інформації, сканування та проникнення

Лабораторне заняття 3. Механізми захисту мережі від збору інформації, сканування та проникнення

Навчальна мета заняття: навчитися користуватися механізмами захисту мережі від збору інформації, сканування та проникнення

Кількість годин: 6 год.

Навчальні питання

1. IDS Snort
2. Персональний міжмережний екран Iptables

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику механізмам захисту мережі від збору інформації, сканування та проникнення. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №5. Застосування криптографічних сервісів

Лабораторне заняття 4. Інфраструктура відкритих ключів

Навчальна мета заняття: навчитися встановлювати і настроювати інфраструктур відкритих ключів

Кількість годин: 6 год.

Навчальні питання

1. Інфраструктура відкритих ключів (PKI)
2. Створення підписаного повідомлення
3. Налаштування веб-серверу з автентифікацією клієнтів за допомогою сертифікатів

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику інфраструктури відкритих ключів (PKI). Вказати спосіб встановлення і використання сервісів.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №6. Аналіз трафіку в комп'ютерних мережах

Лабораторне заняття 4. Аналіз трафіку в комп'ютерних мережах

Навчальна мета заняття: навчитися користуватися інструментами аналізу трафіку в комп'ютерних мережах

Кількість годин: 6 год.

Навчальні питання

1. Перехоплення трафіка
2. MAC затоплення (MAC flooding)
3. ARP Spoofing
4. Атаки на DHCP
5. Підроблений DHCP сервер

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проєктор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам аналізу трафіку в комп'ютерних мережах. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проєктору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №7. Перехоплення сесій передачі даних в комп'ютерних мережах

Лабораторне заняття 5. Перехоплення сесій передачі даних в комп'ютерних мережах

Навчальна мета заняття: навчитися користуватися інструментами перехоплення сесій передачі даних в комп'ютерних мережах при тестуванні безпеки

Кількість годин: 6 год.

Навчальні питання

1. Використання Ettercap
2. Використання Xplico
3. Перехоплення сесії за допомогою Hamster та Ferret

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проєктор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам аналізу трафіку в комп'ютерних мережах. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №8. Безпека в безпроводних мережах

Лабораторне заняття 6. Безпека в безпроводних мережах

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки безпроводних комп'ютерних мереж

Кількість годин: 6 год.

Навчальні питання

1. Аналіз безпроводних мереж
2. Злам безпроводних мереж
3. Засоби прискорення підбору пароллю

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику технології WiFi та напрямам тестування безпеки безпроводних комп'ютерних мереж. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №9. Безпека в операційних системах

Лабораторне заняття 7. Безпека в операційних системах

Навчальна мета заняття: навчитися користуватися інструментами тестування безпеки операційних систем

Кількість годин: 6 год.

Навчальні питання

1. Metasploit framework
2. MetasploitHelper

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику Metasploit Framework та видам атак на парольний захист ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №10. Шкідливе програмне забезпечення

Лабораторне заняття 8. Шкідливе програмне забезпечення

Навчальна мета заняття: навчитися користуватися інструментами створення шкідливого програмного забезпечення для тестування антивірусних систем

Кількість годин: 4 год.

Навчальні питання

1. Створення троянів
2. Протидія і виявлення
3. Створення та аналіз шкідливого коду для Android

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику способам і інструментам створення шкідливого програмного забезпечення, принципам роботи антивірусних систем. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №11. Переповнення буферу

Лабораторне заняття 9. Переповнення буферу

Навчальна мета заняття: навчитися аналізувати вразливість переповнення буферу

Кількість годин: 4 год.

Навчальні питання

1. Аналіз коду програми
2. Усунення вразливості переповнення буферу

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проєктор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику вразливості переповнення буферу. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проєктору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №12. Безпека веб-серверів та веб-застосувачів

Лабораторне заняття 10. Безпека веб-серверів та веб-застосувачів

Навчальна мета заняття: навчитися користуватися інструментами дослідження вразливостей веб-сервера

Кількість годин: 6 год.

Навчальні питання

1. Програмні засоби дослідження вразливостей веб-сервера
2. Атаки на паролі веб-застосувачів
3. Використання вразливостей у ПЗ ОС та веб-сервера

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проєктор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику вразливості переповнення буферу. Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проєктору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №13. Атака «відмова в обслуговуванні»

Лабораторне заняття 11. Атака «відмова в обслуговуванні»

Навчальна мета заняття: навчитися користуватися інструментами атак «відмова в обслуговуванні» при дослідженні безпеки веб-сервера

Кількість годин: 4 год.

Навчальні питання

1. SYN flood атаки
2. Атака на веб-сервер
3. Slowhttptest атаки

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику атак «відмова в обслуговуванні». Вказати спосіб встановлення додаткових застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проектору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №14. SQL-ін'єкції

Лабораторне заняття 12. SQL-ін'єкції

Навчальна мета заняття: навчитися користуватися інструментами тестування на можливість SQL-ін'єкції

Кількість годин: 6 год.

Навчальні питання

1. Код, вразливий до SQL-ін'єкцій
2. Використання UNION SELECT
3. Тестування на можливість SQL-ін'єкції в автоматичному режимі
4. Захист від SQL-ін'єкцій

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проектор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику SQL-ін'єкцій та методам захисту. Вказати спосіб встановлення потрібних застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проєктору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

Тема №15. Соціальна інженерія

Лабораторне заняття 13. Соціальна інженерія

Навчальна мета заняття: навчитися користуватися інструментами створення фішингових сайтів для тестування методів захисту

Кількість годин: 4 год.

Навчальні питання

1. The Social-Engineer Toolkit
2. Ngrok
3. Trape
4. Weeman

Література: Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.

Матеріально-технічне забезпечення: комп'ютерна мережа із підключенням до Internet; медіа проєктор.

План проведення заняття

I. Порядок проведення вступу до заняття.

Дати коротку характеристику методам створення фішингових сайтів та методам протидії фішингу. Вказати спосіб встановлення потрібних застосунків в ОС.

II. Порядок проведення основної частини заняття.

Здобувачі вищої освіти згідно керівництва до практичних та лабораторних занять за темою виконують задачі навчальних питань.

Викладач також синхронно виконує задачі заняття із виводом зображення монітору на екран проєктору.

У ході заняття викладач надає потрібну допомогу та пояснює окремі елементи задач.

III. Порядок проведення заключної частини заняття.

Перевірити у декількох здобувачів результати виконання поставлених задач, виставити відповідні оцінки. Зазначити перелік задач для самостійної роботи, вказати час і спосіб перевірки результатів самостійної роботи.

Оголосити тему наступного заняття.

3. Рекомендована література (основна, допоміжна), інформаційні ресурси в Інтернеті **Основна**

1. Кібербезпека для спеціальних агентів кіберполіції (лекції). OSCE. 2016.
2. Кібербезпека для спеціальних агентів кіберполіції (практика). OSCE. 2016.
3. Matt Walker. CEH Certified Ethical Hacker All-in-One Exam Guide. McGraw-Hill, 2012.
4. ITU-T Rec. X.805. Security architecture for systems providing end-to-end communications./ ITU-T Recommendation X.805, 10/2003. URL: <https://www.itu.int/rec/T-REC-X.805-200310-I/en>(датазвернення: 20.09.2016).

Допоміжна

5. ITU-T Rec. X.800. Security architecture for Open Systems Interconnection for CCITT applications. / Recommendation X.800, Geneva, 1991. URL: <http://www.itu.int/rec/T-REC-X.800-199103-I> (дата звернення: 20.09.2016).
6. ITU-T E.408. Telecommunication networks security requirements. / ITU-T Recommendation E.408, 05/2004. URL: <https://www.itu.int/rec/T-REC-E.408-200405-I/en> (дата звернення: 20.09.2016).
7. NIST Special Publication 800-33. Underlying Technical Models for Information Technology Security. / Gary Stoneburner. CODEN: NSPUE2, December 2001. URL: <http://csrc.nist.gov/publications/nistpubs/800-33/sp800-33.pdf> (дата звернення: 20.09.2016).

Інформаційні ресурси

8. <http://www.hackerhighschool.org/>
9. <https://securityonline.info/>
10. <https://kali.tools/>
11. <https://tools.kali.org/>
12. <https://hackersonlineclub.com/>
13. <https://hakin9.org/>
14. <https://gbhackers.com/>
15. <https://securityonline.info/>
16. <https://www.hackingarticles.in/>