

ADVANCED

CORPORATE SECURITY ARCHITECTURE

OSINT

CYBERSECURITY

INTRO: CYBERSECURITY TOPIC OVERVIEW

SOC ANALYST

SECURITY ENGINEER

MALWARE ANALYSIS

BLUE TEAM

MALWARE DEVELOPMENT

NETWORKING

REVERSE ENGINEERING

RED TEAM

CYBERSECURITY TOOLS

CODING IN CYBERSEC

WEB PENTESTING

IS AUDIT

THREAT HUNTING

INTERNAL PENTESTING

SOCIAL ENGINEERING

MALWARE DEVELOPMENT

SETTING UP A LINUX ENVIRONMENT

TRAFFIC, MALWARE, MEMORY DUMPS

MOBILE PENTESTING

ADVANCED CYBERSECURITY

05/10 INTRO: CYBERSECURITY TOPIC OVERVIEW

Знайомство з основними напрямками в галузі. Хто такі "сині" і "червоні", і чим вони займаються? Pozнайомимося з аудиторами, криптографами, регуляторами та іншими ключовими термінами. Дізнаємося, хто є "білими", "сірими" і "чорними". Обговоримо, що ми будемо робити разом протягом наступного року.

12/10 BLUE TEAM

Blue Team, або напрям інженера з інформаційної безпеки. Які бувають посади та напрямки? Чим займається Security Engineer? Як стати достатньо blue?

19/10 MALWARE ANALYSIS

Зануримося в світ malware analysts — експертів, що "копаються" в шкідливих програмах. Вони використовують круті тулзи для виявлення, аналізу та ліквідації вірусів та троянів. Розглянемо реальні кейси, від того, як вони ловлять "баги", до того, як "роззброюють" їх.

29/10 SECURITY ENGINEER

Security Engineer, або якщо читати в зворотньому порядку. Основні задачі інженера з інформаційної безпеки, як ним стати та що в себе включає це поняття.

ADVANCED CYBERSECURITY

02/11 SOC ANALYST

SOC Analysts — справжні цифрові вартіві. Ті, хто тримає руку на пульсі мережі, виявляючи та відбиваючи кібератаки. З'ясуємо, як вони використовують техніки для моніторингу "traffic" та "alerts", і що треба знати, щоб стати одним з них. Розглянемо кілька крутих кейсів із реального життя.

09/11 NETWORKING PART 1

Ця лекція покриває основи networking. Ми розберемо, як знання про мережі допоможе вам у майбутньому, особливо коли мова йде про "червоних" хакерів.

16/11 NETWORKING PART 2

Тема складна, тому ця лекція для глибшого розуміння ключових концепцій і технік. Ми поглибимо наші знання про протоколи, маршрутизацію та комутацію, з особливим акцентом на техніки.

14/12 CODING IN CYBERSEC

Готуйтеся познайомитися з кодуванням у кібербезпеці! Розберемося, які мови програмування є must-have для хакерів і захисників. Поговоримо про основні прийоми і техніки, що допомагають "script kiddies" стати професіоналами.

ADVANCED CYBERSECURITY

21/12 SETTING UP A LINUX ENVIRONMENT

Теорія про "блу" уже за плечима, настав час для практики! Ставимо віртуальну машину, завантажуємо необхідні інструменти, і занурюємося у світ Linux. Навчимося основам: від базових команд до розуміння того, як працює система.

11/01 TRAFFIC, MALWARE, MEMORY DUMPS

Час зануритися у практичне використання інструментів кібербезпеки. У цій лекції ми аналізуємо трафік, виявляємо малвар і розбираємося з дампами пам'яті.

18/01 CORPORATE SECURITY ARCHITECTURE

Зануримося в бест практики "блу" та вивчимо, як будувати надійну архітектуру безпеки для корпорацій. Поглянемо на ключові елементи, які тримають захист на високому рівні, від firewalls до encrypted networks.

25/01 RED TEAM

Заглянемо за лаштунки "червоних" – тих, хто розбирає захист на шматки, імітуючи атаки. Обговоримо ключові навички та інструменти, які вони використовують, щоб виявити прогалини в безпеці. Розберемося в тому, як з набором потужних skills можна заслужити репутацію гуру в атаках "червоного" кольору.

ADVANCED

CYBERSECURITY

01/02 CYBERSECURITY TOOLS

У цій лекції ми зберемо всі круті тулзи, які вам знадобляться для наступних практик. Покажемо, як налаштувати кіберзброю для захисту, відстеження та аналізу.

Готуйтеся до глибокого занурення в кібер-екіпірування.

08/02 WEB PENTESTING

Ця лекція занурить вас у світ веб пентест. Вчимося, як "ламати" сайти, щоб тестувати їхню безпеку. Розглянемо типові вразливості, які допоможуть вам стати крутим веб-хакером. Готуйтеся до екшну з кодом та запитам!

15/02 PRACTICAL SESSION: WEB PENTESTING

Занурюємось в активне веб пентест з використанням платформ HTB (Hack The Box) та THM (TryHackMe). Вивчимо, як виявляти слабкі місця на живих сайтах і застосовувати техніки безпеки в дії.

22/02 INTERNAL PENTESTING OVERVIEW

Заглиблюємося в пентест внутрішніх мереж і систем. Покажемо, як "вишукувати" і латати діри в безпеці вашої організації. Дізнаєтеся про круті тулзи та трюки, які допомагають тримати корпоративні дані під замком. Готові зануритися в глибину ваших мереж і зрозуміти, що до чого?

ADVANCED

CYBERSECURITY

01/03 HANDS-ON INTERNAL PENTESTING

Запускаємо практичний внутрішній пентест з HTB і THM! Готуйтеся до крутих задач, де ви "відпрацьовуватимете" на власних мережах. Вчимося виявляти та фіксувати "баги" прямо на ходу.

08/03 SOCIAL ENGINEERING

Ця лекція розкриває тему соціальної інженерії — тактики, яку хакери використовують для обману людей, щоб отримати доступ до інформації. Вивчимо основні методи, які вони використовують для маніпуляції, включаючи фішинг, вейлінг та бейтинг.

15/03 OSINT

Заглибимося в OSINT, де ви навчитеся "видобувати" інфо з відкритих ресурсів як справжній кібер-детектив. Вчимося трекати важливі дані через соцмережі, вебсайти та інші публічні місця.

22/03 MALWARE DEVELOPMENT

Пірнаємо у базову розробку малвару! Ознайомимося з основними фішками та техніками, які використовуються для бастування шкідливого софту. Пройдемося по різних типам малвару, вивчимо, чому і як вони "живуть" у системах. Також обговоримо, як це все виглядає з точки зору етики та закону. Загрузимо в темну сторону кодингу!

ADVANCED CYBERSECURITY

29/03 MALWARE DEVELOPMENT

Забираємося глибше у світ шкідливих програм! Навчимося бастувати малвар використовуючи популярні тулзи та мови програмування. Розглянемо, як тестувати і аналізувати наші шкідливі "творіння" у контрольованому середовищі.

05/04 REVERSE ENGINEERING

Зануримося в реверс-інжиніринг, де ми вчитимемося "розшифровувати" все, від софта до харду. Дізнаємося, як вичленити бінарники та зрозуміти, як програми функціонують. Ви навчитеся "читати" техніку, відкриваючи секрети, заховані в коді та схемах.

12/04 RED TEAM WRAP-UP

Завершуємо наш "ред" марафон! Підбиваємо підсумки всього, що вивчили. Разом переглянемо, як усі знання та інструменти зливаються в єдину стратегію безпеки.

19/04 IS AUDIT

*ануримося в світ аудиту інформаційної безпеки. Дізнаємося, що таке аудит ІБ і чому він критично важливий для будь-якої організації. Поговоримо про основні задачі аудиторів: від оцінки ризиків до виявлення "лазівок" в системах. Також обговоримо, які навички та кроки потрібні, щоб увійти в цей світ кібер-захисту.

ADVANCED CYBERSECURITY

10/05 THREAT HUNTING

Вивчаємо арт Threat Hunting — активний пошук та нейтралізація кіберзагроз, які ще не "спіймані" автоматичними системами. Дізнаємось, як "вираховувати" небезпеку, використовуючи круті методи та інструменти.

17/05 MOBILE PENTESTING

Зануримося у світ пентесту мобільних девайсів! Розберемо, з якими викликами та підступами можна зустрітися в мобільному світі і як "крашити" вразливості на iOS та Android. Подивимось, які тулзи перемагають у мобільному пентестінгу і як їх використовувати, щоб кожен додаток пройшов жорсткий кібер-тест на міцність.