

В Linux можна оновлювати всі системні програми з однією командою в терміналах.

Windows – дуже простий в установці та використанні, але його неможливо змінити. Необхідно встановлювати антивірусне програмне забезпечення, потрібно регулярно його оновлювати. Навіть хороший антивірус менш надійний, ніж Linux. Windows потребує великої кількості апаратних ресурсів, а також використовує пропускну здатність в антивірусному оновленні тощо.

Переваги KaliLinux. Наявні близько 600 інструментів: KaliLinux має велику колекцію інструментів тестування на проникнення; багатомовна підтримка; за допомогою KaliLinux кіберполіцейські можуть оцінити обчислювальну інфраструктуру хакерів, виявляти уразливості та цифрові сліди.

За допомогою KaliLinux можуть бути використані деякі кроки для тестування, проникнення та фіксації дії хакерів. Наприклад – розвідка, у цьому процесі кіберполіцейський збирає попередню інформацію про протиправні дії, це дає змогу краще планувати атаку. Потім – сканування, на цьому кроці використовуються технічні засоби для збору додаткової інформації про ціль, за допомогою сканера вразливостей для виявлення лазівки в безпеці цільової мережі. Деякі інструменти сканування та види атак у KaliLinux включають в себе ARP-сканування, ін'єкції JSQ, інструмент Cisco-аудит. Після чого – отримання доступу, на цьому етапі можливо проводити дії на цільовій мережі з метою вилучення деяких корисних даних для запуску додаткових атак. Деякі інструменти KaliLinux дозволяють здійснювати підтримку доступу. Крім того існують інструменти, що усувають будь-які ознаки минулої шкідливої активності в цільовій мережі. Наприклад, будь-які внесені зміни або збільшення доступу до прав, повертаються в їх вихідний статус.

Підбиваючи підсумки сказаному можна резюмувати KaliLinux є потужним інструментом для тестування на проникнення для спеціалістів з інформаційної безпеки. Користуючись KaliLinux, можна належним чином захистити критичну ІТ-інфраструктуру від зловмисників. KaliLinux дозволяє виконувати додаткові тестування на проникнення, щоб виявляти уразливості у вашій мережі.

Одержано 22.04.2019



УДК 343.98(477)

Данило Олександрович КУЛІКОВ,

курсант групи Ф4-302 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАСТОСУВАННЯ СПЕЦІАЛЬНОЇ ТЕХНІКИ ПІД ЧАС ПРОВЕДЕННЯ НЕГЛАСНИХ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ

Згідно з главою 21 «Негласні слідчі (розшукові) дії» Кримінального процесуального кодексу України до негласних слідчих (розшукових) дій (далі – НСРД) належать, зокрема, НСРД, пов'язані із втручанням у приватне

спілкування. До таких дій кримінальним процесуальним законодавством України віднесено:

1. аудіо-, відеоконтроль особи (ст. 260 КПК України);
2. накладення арешту на кореспонденцію (ст. 261 КПК України);
3. огляд і виймка кореспонденції (ст. 262 КПК України);
4. зняття інформації з транспортних телекомунікаційних мереж (ст. 263 КПК України);
5. зняття інформації з електронних інформаційних систем (ст. 264 КПК України);
6. обстеження публічно недоступних місць, житла чи іншого володіння особи (ст. 267 КПК України);
7. установлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України);
8. спостереження за особою, річчю або місцем (ст. 269 КПК України);
9. аудіо-, відеоконтроль місця (ст. 270 КПК України);
10. контроль за вчиненням злочину (ст. 271 КПК України);
11. виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (ст. 272 КПК України);
12. негласне отримання зразків, необхідних для порівняльного дослідження (ст. 274 КПК України).

Відомо, що під час проведення будь-яких негласних слідчих (розшукових) дій на практиці фактично використовуються технічні пристрої та засоби, або інформаційні технології у вигляді обчислювальної техніки та відповідного програмного забезпечення, що найчастіше викликають ускладнення під час використання. Якщо проведення таких НСРД, як аудіо-, відеоконтроль особи чи місця, обстеження публічно недоступних місць, житла чи іншого володіння особи або спостереження за особою, річчю чи місцем не викликає складнощів, то зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем може суттєво ускладнити або унеможливити проведення досудового розслідування. Тому виникає необхідність підвищення якості знань працівників поліції у вказаних галузях та інформаційних технологіях.

Використання сучасних технічних засобів і пристроїв під час проведення негласних слідчих (розшукових) дій, може значно покращити ефективність та якісні показники проведення НСРД. Зокрема, це: цифрові дзеркальні наддовгофокусні фотоапарати або відеокамери; фотоапарати або відеокамери з режимом нічний зйомки; пристрої нічного бачення; портативні рентгенівські сканери; пристрої прихованої аудіо- та відеофіксації; сучасні радіосканери.

Які конкретно технічні засоби необхідно використовувати у вказаних негласних слідчих (розшукових) діях – слід вирішувати слідчому, якщо він проводить їх особисто, чи узгоджувати з працівниками технічних й інших оперативних підрозділів, яким доручено виконувати проведення негласних слідчих (розшукових) дій. Такі знання слід мати для орієнтування щодо можливостей

вказаних сучасних технічних досягнень і для запровадження у практичну діяльність Національної поліції.

Одержано 18.04.2019



УДК 343.9

Роман Русланович ОРЛОВ,

курсант групи Ф4-102 ХНУВС

Науковий керівник: кандидат технічних наук, доцент Світличний В. А.

ЗАСТОСУВАННЯ ПОЛІГРАФА В ДІЯЛЬНОСТІ ПОЛІЦІЇ

Достовірність досліджень з використанням поліграфа безпосередньо залежить від умінь поліграфолога та його наукового і практичного базису. Сертифікованих поліграфологів готують виключно в навчальних закладах. Експерт-поліграфолог це професія, яка офіційно була затверджена ще в 2010 році у Національному класифікаторі професій України (код професії – 2144.2), але зараз існує велика кількість приватних шкіл і поліграфологів, які, не маючи ліцензії на освітні послуги, пропонують сумнівні курси з навчання навикам роботи з поліграфом.

У сфері правоохоронної діяльності поліграф використовують, згідно з Інструкцією про порядок використання поліграфів у Національній поліції України яка затверджена наказом МВС України від 13.11.2017 № 920, у наступних випадках: під час вступу кандидатів на службу до поліції; у разі проведення атестування поліцейських; перевірка з власної ініціативи особи, яка виявила бажання бути опитаною з використанням поліграфа, у тому числі під час проведення службових розслідувань; здійснення оперативно-розшукової діяльності і багатьох інших випадках.

При створенні Національної поліції України можливість використання поліграфів була закріплена на рівні законодавства, а саме згідно з ч. 2 ст. 50 (перевірка кандидата на службу в поліції) Закону України «Про Національну поліцію» «громадяни України, які виявили бажання вступити на службу в поліції, за їхньою згодою проходять тестування на поліграфі».

Також поліграф можуть використовувати не тільки для розслідування злочинів та відбору персоналу, але й у напрямі організації моніторингу за принципом зворотного зв'язку при навчанні персоналу поліції навичкам психологічної саморегуляції, клінічної експертизи наявності у співробітника поліції посттравматичного стресового розладу, психолого-фізіологічної діагностики агресивності і тривожності особистості та інше.

Поліграф сприяє більш глибокому і ретельному вивченню людини, ніж всі інші методи, які можуть використовувати в роботі фахівці, тому поліція України повинна бути оснащена поліграфами. Причому ці пристрої повинні мати більш високими технічними характеристиками, що дозволить мати