Список бібліографічних посилань

1. Кримінальний процесуальний Кодекс України : закон України від 13.04.2012 № 4651-VI // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 30.11.2018).

2. Про внесення змін до Господарського процесуального кодексу України, Цивільного процесуального кодексу України, Кодексу адміністративного судочинства України та інших законодавчих актів : закон України від 03.10.2017 № 2147-VIII // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/2147-19 (дата звернення: 30.11.2018).

3. Цехан Д. М. Цифрові докази: поняття, особливості та місце в системі доказування. *Науковий вісник Міжнародного гуманітарного університету*. 2013. № 5. URL: http://nbuv.gov.ua/UJRN/Nvmgu_jur_2013_5_58 (дата звернення: 30.11.2018).

4. Зигура Н. А., Кудрявцева А. В. Компьютерная информация как вид доказательств в уголовном процессе России : моногр. М.: Юрлитинформ, 2011. 176 с.

5. Васильєв С. В., Ніколенко Л. М. Доказування та докази у господарському процесі України : моногр. Х. : Еспада, 2004. 192 с.

6. Зайцев П. П. Допустимость в качестве судебных доказательств фактических данных, полученных с использованием электронных документов. *Арбитраж и гражд. процесс.* 2002. № 4.

Одержано 30.11.2018

УДК 332.012+004.056.5

Ксенія Олександрівна КРАТАСЮК,
курсант 3 курсу групи Ф4-302 факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ;
Денис Олександрович ГРИЩЕНКО,
старший викладач кафедри кібербезпеки факультету № 4 (кіберполіції) Харківського національного університету внутрішніх справ

KALI LINUX ЯК ПОТУЖНА ЗБРОЯ КІБЕРЗЛОЧИНЦІВ

На сьогоднішній день дистрибутив Kali Linux набирає велику популярність. Злом і тестування безпеки стає частиною нашої культури і все більше людей цікавляться цим. Kali Linux розроблений як для хакерів так і фахівців з безпеки захисту інформації.

Linux як форма поширення програмного забезпечення – це не більше ніж ядро і набір базових утиліт, програм і налаштувань за замовчуванням. Kali Linux не надає нічого унікального в цьому плані.

Відмінність Kali Linux в тому, що він наповнений такими інструментами і настройками, які потрібні для тестування безпеки, а не для забезпечення нормальної роботи звичайного користувача. Використовуючи Kali замість основної форми розповсюдження програмного забезпечення – помилка. Це спеціалізований дистрибутив

для вирішення певного кола завдань. Можливості Kali Linux зосереджені на тестуванні безпеки, що також може бути використано хакерами з метою пошуку вразливостей у вашій системі.

Відмінності Linux від Windows

Linux – відкритий та безкоштовний, ніякого вірусу чи шкідливого програмного забезпечення, не потрібно платити за антивірусне програмне забезпечення, яке споживає багато системних ресурсів і робить ваш ПК повсякденним і потребує регулярного оновлення. Не потрібно заходити в Інтернет і шукати індивідуальний пакет. Більшість Linux Distribution має власний центр програмного забезпечення, з якого можна легко його встановити. 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. Щоб встановити програмне забезпечення потрібно знайти його онлайн, завантажити потім встановити. Іноді доведеться вручну видаляти старе програмне забезпечення, перш ніж оновити його. Навіть хороший антивірус менш надійний, ніж Linux. Windows потребує великої кількості апаратних ресурсів, а також використовує пропускну здатність в антивірусному оновленні тощо.

Особливості Kali Linux:

– наявні близько 600 інструментів: Kali Linux має велику колекцію інструментів тестування на проникнення;

– повністю безкоштовний;

– багатомовна підтримка;

– цілковито налаштований: ніщо не перешкоджає переробляти інструмент відповідно до дизайнерських потреб, навіть від ядра;

– підтримка ARMEL та ARMHF;

– модель із відкритим кодом: дає змогу налаштувати свій вихідний код в Kali Linux.

За допомогою Kali Linux, хакери можуть оцінити обчислювальні інфраструктури організації та виявляти уразливості, які вони можуть використати в своїх цілях.

Основні кроки для тестування на проникнення в мережу Kali Linux, які можуть бути використані хакерами.

1. Розвідка

У цьому процесі хакер збирає попередню інформацію про ціль, це дає змогу краще планувати атаку.

Деякі засоби розвідки Kali Linux включають в себе:

– Recon-ng;

– Nmap;

– Hping3;

– DNSRecon.

2. 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 Kali Linux включають в себе:

– ARP-сканування;
– ін'єкції jSQL;
– інструмент Cisco-аудит;
– Oscanner;
– WebSploit.

3. Отримання доступу

На цьому етапі хакер проводить дії на цільовій мережі з метою вилучення деяких корисних даних або використання скомпрометованої системи для запуску додаткових атак.

Деякі інструменти експлуатації Kali Linux включають в себе:

– Metasploit Framework;
– BeEF (платформа експлуатації браузера);
– Wireshark;
– Aircrack-ng.

4. Підтримка доступу

Деякі інструменти Kali Linux для підтримки доступу включають в себе:

– Powersploit;
– Webshells;
– Dns2tcp.

5. Прикриття слідів

На цьому останньому етапі хакер усуває будь-які ознаки минулої шкідливої активності в цільовій мережі. Наприклад, будь-які внесені зміни або збільшення доступу до прав, повертаються в їх вихідний статус.

Деякі інструменти Kali Linux для обробки payload (корисних навантажень):

– Meterpreter;
– Smbexec.

Висновок. Kali Linux в кібербезпеці є потужним інструментом для тестування на проникнення як для хакерів так і для спеціалістів з інформаційної безпеки. Користуючись цим інструментом, можна належним чином захистити критичну IT-інфраструктуру від зловмисників. Можна виконувати додаткові тестування на проникнення, щоб виявляти уразливості у вашій мережі.

Список бібліографічних посилань

1. Піскозуб А. З. Використання вільного програмного забезпечення для підвищення рівня захищеності комп’ютерних мереж та систем // Матеріали другої міжнародної науково-практичної конференції «FOSS Lviv 2012». Львів, 2012. С. 86-90.

2. Kali Linux. URL: http://www.kali.org/ (дата звернення: 30.10.2018).

3. Стефінко Я. Я., Піскозуб А. З. Використання відкритих операційних систем для тестування на проникнення в навчальних цілях. *Вісник Національного університету «Львівська політехніка»*. Комп'ютерні системи та мережі. 2014. № 806. С. 258-263. URL: http://nbuv.gov.ua/UJRN/VNULPKSM_2014_806_41 (дата звернення: 30.10.2018).

4. Різниця між Windows, Linux і Mac // Моя освіта – реферати, конспекти, доповіді. 30.01.2016 URL: http://moyaosvita.com.ua/tehnologii/riznicya-mizh-windows-linux-i-mac/ (дата звернення: 30.10.2018).

Одержано 02.11.2018

УДК 343.415

Тетяна Петрівна МАТЮШКОВА,
кандидат юридичних наук, доцент,
доцент кафедри криміналістики та судової експертології
факультету № 1 (слідства)
Харківського національного університету внутрішніх справ;
ORCID: https://orcid.org/0000-0001-7973-4581

ВИКОРИСТАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ПРИ ВЧИНЕННІ ОКРЕМИХ ВИДІВ ЗЛОЧИНІВ ПРОТИ ВИБОРЧИХ ПРАВ ГРОМАДЯН

Компанії Google, Facebook та Twitter заявили про використання своїх серверів для розповсюдження дезінформації під час передвиборчої кампанії президента США, що могло суттєвим чином вплинути на результати виборів. За повідомленнями у засобах масової інформації, у листопаді цього року у Конгресі США заплановані слухання відносно незаконного втручання у вибори, у зв'язку з чим представники зазначених кампаній викликані для дачі показань [1]. Про вплив ботів і фейків на вибори у Німеччині свідчать дослідження Оксфордського університету [2].

Використання інформаційних технологій при вчиненні злочинів проти виборчих прав громадян має місце й в Україні. Зокрема, у квітні 2014 р. прес-центр Служби безпеки України повідомляв про виявлення та припинення значної кількості хакерських атак на офіційний веб-сайт ЦВК і систему «Вибори» [3]. За період чергових місцевих виборів 2015 року Національною поліцією було розпочато 478 досудових розслідувань за статтями 157-160 Кримінального кодексу України (далі – КК України), якими встановлюється відповідальність за злочини проти виборчих прав громадян. Майже 16% з яких (78 кримінальних проваджень) стосувались, зокрема, надання неправдивих відомостей до органу ведення Державного реєстру виборців або фальсифікація виборчих документів, документів