1. Server Roles and Technologies in Windows Server 2012 R2 and Windows Server 2012 [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://technet.microsoft.com/en-us/library/hh831669(v=ws.11).aspx (дата звернення 12.10.2017) – Назва з екрана.

2. Security Policy Settings Reference [Електронний ресурс] : [Веб-сайт]. – Електронні дані. – Режим доступу: https://technet.microsoft.com/en-us/library/dn452423(v=ws.11).aspx (дата звернення 12.10.2017) – Назва з екрана.

Методики та інструменти аудиту кібербезпеки інформаційних систем.

Махницький О.В.
старший викладач кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

У повсякденному житті часто інформаційна безпека (ІБ) розуміється лише як необхідність боротьби з витоком секретної та поширенням неправдивої і ворожої інформації. Однак, це розуміння дуже вузьке. Існує багато різних визначень інформаційної безпеки, в яких висвічуються окремі її властивості. Під інформаційною безпекою розуміється стан захищеності інформаційного середовища суспільства, що забезпечує її формування та розвиток в інтересах громадян, організацій і держави.

В інших джерелах наводяться наступні визначення:

Інформаційна безпека - це

1) комплекс організаційно-технічних заходів, що забезпечують цілісність даних і конфіденційність інформації в поєднанні з її доступністю для всіх авторизованих користувачів;

2) показник, що відображає статус захищеності інформаційної системи;

3) стан захищеності інформаційного середовища;

4) стан, що забезпечує захищеність інформаційних ресурсів і каналів, а також доступу до джерел інформації.

Існує кілька підходів до тестування кібербезпеки інформаційних систем.

Термін «інформаційна безпека» часто трактується як шифрування інформації. Ця область зазвичай регулюється державними та відомчими нормативними актами. Проблема такого підходу полягає в його статичності. Крім того, вона охоплює лише частину питань, пов'язаних з кібербезпекою. Кожну хвилину хакери працюють над новими прийомами несанкціонованого доступу, а норми і методики перевірки стійкості до кіберзагрозам залишаються незмінними на протязі багатьох років. У зв'язку з цим виникають питання:

Наскільки мережа захищена від несанкціонованого вторгнення ззовні? Наскільки актуальні методології та інструменти аудиту мережевої кібербезпеки? Крім того, в інформаційну безпеку можуть входити питання продуктивності мережевого обладнання: ті чи інші класи мережевих пристроїв повинні не тільки перешкоджати вторгненню ззовні в вашу мережу, а й безперешкодно пропускати корисний трафік, не заважаючи нормальній роботі організації.

Існують інструменти та методики, що дозволяють по-новому поглянути і оцінити ступінь захисту інформаційних ресурсів і мережевих вузлів.

Що є об'єктом тестування (аудиту)? Тестується стійкість мережевої інфраструктури і додатків до широкого спектру кібератак з застосуванням новітніх методик і апаратних засобів. Об'єктами тестування на предмет інформаційної безпеки і стійкості до кібератаки є:

• Периметри інформаційної безпеки

• Критична мережева інфраструктура (магістральні маршрутизатори, комутатори, NAT), в тому числі на об'єктах стратегічного значення

• Центри обробки даних (ЦОД)

• Мережеві додатки і сервіси

• Машинні системи, об'єднані в мережі (IoT - т.зв. «інтернет речей»)

• Роботизовані системи, в тому числі:

- промислові

- військові, включаючи безпілотні системи

• Бортові інформаційні системи (авіоніка) літаків, морських суден, автомобілів і т.д.

Типовими об'єктами для тестів інформаційної безпеки є маршрутизатори, балансувальник трафіковий навантаження, міжмережеві екрани, комутатори, програмно-апаратні комплекси для глибокого аналізу трафіку, що проходить (DPI), ЦОДи, а також різні комбінації включення цих пристроїв.

Існують спеціальні апаратні рішення призначені для аудиту стійкості мережевої інфраструктури і додатків до існуючих і перспективних кіберзагрозам, включаючи: стресове навантаження, різні DDoS-атаки, шкідливий код в загальному трафіку, спам, черви, атаки типу «zero day», атаки із застосуванням технології fuzzing , і т.д.

Випробування на інформаційну безпеку проводяться в лабораторних умовах - тобто нема на працюючої мережі. Для цього використовується досліджуваний пристрій (DUT - device under test), або цілий фрагмент мережі в зборі (SUT - system under test) і спеціальний генератор / аналізатор трафіку, який створює стресову навантаження з корисного і шкідливого трафіку і одночасно аналізує відгук від досліджуваного пристрою або системи.

Переваги даного методу полягає в можливості генерації і аналізу стресового навантаження (трафіка) і одночасному аналізі якості роботи інформаційної системи по різним метрик якості та сприйняття інформаційних сервісів (QoS / QoE).

Апаратне рішення тестової складової - генератор стресового навантаження. Генератор стресового навантаження є спеціальним програмно-апаратним комплексом. Його мета - створити стресовий потік трафіку високої щільності на рівнях L2-L7 (по моделі OSI) і проаналізувати відгук і поведінку досліджуваного об'єкта при різних рівнях навантаження і профілях мережевого трафіку. Пристрій емулює запити великої кількості користувачів з унікальними IP-адресами, а також сервери додатків.

Даний комплекс заходів призначений для тестування на стійкість мережевої інфраструктури і додатків до шкідливого трафіку, включаючи:

- Різні типи DDoS-атак
- Черви
- Fuzzing
- E-mail атаки
- Віруси / Трояни / Malware (такі як Red October і т.д.)
- VoIP-атаки
- Атаки на додатки
- Evaded Attacks / Fragmentation

- Сканування і порушення роботи портів
- Buffer Overflows / Protocol Exploitation
- Генерація flooding-атак з інтенсивністю до декількох мільйонів в секунду
- Комбіновані і багатоступінчасті атаки

• Пошук вразливостей в інфраструктурі і додатках для несанкціонованого проникнення ззовні (хакерський взлом) і zero-day атаки

• Вибір технічних рішень і постачальників

• Розробка засобів інформаційного захисту

• Налаштування політик периметрів інформаційної безпеки (при зміні прошивок, додаванні нових IT-сервісів, оновлення обладнання і т.д.)

Генеруються атаки постійно підтримуються в актуальному стані за рахунок періодичного поновлення бази даних атак.

Крім цього, користувач може створювати власні атаки за допомогою спеціального конструктора атак (Attack Designer). Атаки можуть бути створені як «з нуля», так і шляхом модифікації наявних бібліотек. Для більшої гнучкості реалізована можливість використання pcap-файлів. Як приклад для інструментів для аудиту периметрів інформаційної безпеки можна розглянути:

Генератор хакерських атак, шкідливого трафіку і корисного прикладного трафіку Spirent Avalanche

Генератор стресового навантаження, змішаного і шкідливого трафіку нового покоління Avalanche NEXT

Приклади тестування інформаційної безпеки з використання зазначених вище інструментів:

• Тестування електричного навантаження на і стійкості web-порталу до DDoS-атакам.

• Тестування продуктивності банківської мережевої інфраструктури по можливості підключення банкоматів по каналах IPSec.

• Налаштування політик безпеки і продуктивності периметра інформаційної захисту організації.

• Тестування стійкості SaaS сервісу в ЦОДі.

• Стресовий тестування RADIUS-сервера в core-мережі оператора мобільного зв'язку.

[Електронний ресурс]. – Режим доступу: http://www.lab.pr-group.ru/ITsecurity.html

[Електронний ресурс]. – Режим доступу: https://uk.wikipedia.org/w/index.php? search=безпеака+інформації

Інформаційна безпека України в сучасних умовах

Мирошниченко В.О.
к. т. н., доцент кафедри економічної та інформаційної безпеки Дніпропетровського державного університету внутрішніх справ

Інформаційна безпека в XXI столітті виходить на перше місце в системі національної безпеки держави, тому лише та держава може розраховувати на лідерство в економічній, військово-політичній та інших сферах, мати стратегічну і тактичну перевагу, гнучкіше регулювати економічні витрати на розвиток озброєнь і військової техніки, підтримувати перевагу з ряду передових технологій, яка має перевагу в засобах інформації та інформаційної боротьби.

Інформація постійно ускладняється, змінюється якісно, зростає кількість її джерел і споживачів. Водночас збільшується і уразливість сучасного інформаційного суспільства від недостовірної (а іноді й шкідливої) інформації, її несвоєчасного надходження, промислового шпигунства, комп'ютерної злочинності й т. ін. Тому Конституцією України забезпечення інформаційної безпеки віднесено до найважливіших функцій держави.

За даними наукових досліджень, система забезпечення інформаційної безпеки України не виконує окремих важливих функцій. Зокрема, неефективними є управління її діяльністю, організаційні зміни, що здійснюються в межах адміністративної реформи, мають несистемний характер, проводяться без попереднього функціонального дослідження органів державної влади. Негативні тенденції розвитку національного інформаційного простору, кризовий стан економіки країни та інші чинники обумовлюють ескалацію загроз, що може призвести (а часом і призводить) до значних втрат політичного, економічного, воєнного та іншого характеру, завдання шкоди юридичним особам та громадянам.