БЕЗПЕКА КОМП'ЮТЕРНИХ МЕРЕЖ ТА ІНТЕРНЕТ / NETWORK & INTERNET SECURITY

ТЕХНОЛОГІЯ ВИКОРИСТАННЯ УРАЗЛИВОСТЕЙ WEB РЕСУРСІВ У ПРОЦЕСІ ОРГАНІЗАЦІЇ ТА ПРОВЕДЕННЯ МЕРЕЖЕВОЇ РОЗВІДКИ ІНФОРМАЦІЙНО-ТЕЛЕКОМУНІКАЦІЙНИХ СИСТЕМ

Володимир Бурячок

Військова частина А1906, Україна

БУРЯЧОК Володимир Леонідович, д.т.н., с.н.с

Рік та місце народження: 1963 рік, м. Лутугіне, Луганська область, Україна.
Освіта: Київське вище інженерне радіотехнічне училище Протиповітряної оборони імені Маршала авіації О.І. Покришкіна, 1985 рік.
Посада: начальник науково-дослідного управління з 2007 року.
Наукові інтереси: системний аналіз, прийняття рішень та науково-технічне прогнозування, інформаційна і кібербезпека
Публікації: більше 120 наукових публікацій, серед яких монографії, навчальні посібники, бюлетені, наукові статті та тези доповідей.
E-mail: BVL-home@ua.fm

Анотація. *Розглянуто призначення та основні різновиди розвідки інформаційно-телекомунікаційних систем. Запропоновано визначення розвідки у системах телекомунікацій, мережної (МР) та кіберрозвідок. Визначено сферу можливих інтересів МР та метод її ведення, а також місце МР у загальному процесі добування інформації. Розглянуто приклад використання уразливостей Web ресурсів при організації та проведенні МР ІТС.*

Ключові слова: *інформація, інформаційно-телекомунікаційна система, мережева розвідка*

Постановка завдання у загальному вигляді

Науково-технічна революція наприкінці XX початку XXI сторіччя викликала у світі глибокі системні перетворення. Вони, як результат, дали можливість завдяки синтезу перспективних інформаційно-комунікаційних технологій (ІКТ) і бурхливого розвитку електронної обчислювальної техніки сформуватись та розвинутись принципово новим і невід'ємним глобальним субстанціям: інформаційному суспільству, інформаційному простору та його окремій складовій – простору кібернетичному. Неконтрольоване поширення і використання останніх перш за все як сфери ведення воєнних конфліктів сучасності і найближчого майбутнього, зростання впливу засобів масової інформації (ЗМІ), а також впливу ІКТ та інформаційно-телекомунікаційних (ІТ) систем на постіндустріальне суспільство, поява небезпеки розриву між інформаційною елітою та споживачами привело до того, що поряд з отриманням значних переваг від застосування інформаційного та кіберпросторів світове співтовариство набуло й усі пов'язані з ними проблеми. Внаслідок чого:

– суттєво ускладнилось завдання добування даних, що необхідні для прийняття виважених, адекватних умовам обстановки рішень;

– світ став надто уразливим від появи нових деструктивних впливів – викликів, загроз та фактично неприхованих кібернетичних злочинів в ІТ сфері;

– все частіше інформаційний і кіберпростори почали використовуватися як об'єкти інформаційно-технічного та інформаційно-психологічного впливу тощо.

Аналіз останніх досліджень і публікацій

Ці проблеми висвітлено в багатьох публікаціях зарубіжних і вітчизняних авторів. Найвідомішими серед них є роботи А.А. Безбогова, В.В. Дудихіна, С.В. Кузнецова, С.В. Ленкова, А.І. Романова, Н.Р. Ромачова, В.О. Хорошка, О.К. Юдіна, Є. Ющука та інших фахівців. Тим не менш аналіз публікацій у предметній області, що розглядається, свідчить про те, що комплексного

дослідження як питань пошуку інформації про можливості протиборчих сторін у відкритих та її добування з відносно відкритих і закритих електронних джерел, так і питань захисту їх інформаційного і кіберпросторів від стороннього кібервпливу, а також методів які при цьому застосовуються до цього часу не проводилось. Тому вони потребують додаткового і більш глибокого вивчення.

Актуальність та мета статті

Отже, актуальність статті обумовлена насамперед обсягом інформації, що останнім часом надходить до користувачів із зовнішнього середовища та безперервно зростає [1], необхідністю підвищення ефективності засобів пошуку і добування розвідувальних відомостей про об'єкт розвідки із ресурсів ІТ систем (ІТС), а також оцінювання на підставі отриманої інформації можливих загроз власному кіберпростору [2]. Важливою умовою розв'язання означених проблем стає оперування єдиним понятійним апаратом у кібербезпековій сфері та знання специфіки розвідувальних процесів у ІТ середовищі.

Мета статті та її основний зміст полягають у викладенні основних понять та особливостей організації розвідки ІТС й передусім такого способу її ведення, як мережева розвідка (МР), а також технології організації і проведення МР з використанням уразливостей притаманних, наприклад, Web-ресурсам.

Виклад основного матеріалу

Зважаючи на стрімкий технологічний розвиток інформаційного суспільства та нові комунікаційні можливості кількість потенційно можливих як відкритих і відносно-відкритих, так і закритих електронних джерел інформації останнім часом значно розширилась. Це визначило потребу концентрації зусиль за напрямком організації і проведення розвідувальної діяльності в існуючих ІТ системах і мережах та впровадження такого нового виду розвідки , як розвідка ІТС – комплексу заходів, спрямованих на систематичний і цілеспрямований пошук, збір та добування з автоматизованих ІТС, комп'ютерних мереж і систем зв'язку цивільного та/або військового призначення інформації стосовно протиборчої сторони, її вивчення та обробки, а також формування на цій підставі уявлення про реальні та/або потенційно можливі джерела стороннього кібернетичного впливу.

Від інших видів розвідка ІТС відрізняється насамперед механізмами – способами і методами, а також силами і засобами, що задіяні у процесах збору та/або добування інформації [3]. Головними способами її ведення нині вважають розвідку систем телекомунікацій (РСт), мережеву і кіберрозвідку (КР). Як свідчить досвід практичної діяльності підрозділів спецпризначення, результати навчань і тренувань найбільш вагомою за цінністю добутої інформації але одночасно й найменш результативною за кількістю такою інформації у сучасних умовах вважають мережеву розвідку силами й засобами якої добувається до 7% інформації, що необхідна протиборчим сторонам один про одного. На думку вітчизняних і західних фахівців вона є комплексом заходів, спрямованих на систематичний пошук, збір та/або добування даних про ресурси, засоби захисту, пристрої та програмне забезпечення (ПЗ), що використовується в ІТС об'єкта розвідки, їх уразливі місця та межі проникнення з подальшим обліком та накопиченням такої інформації, її верифікацією, вивченням і аналітичною обробкою.

Мережеву розвідку ІТС в ЗМІ доволі часто асоціюють з "конкурентною" або "бізнес" розвідками, тобто з усім тим, що на Заході прийнято називати єдиним терміном competitive intelligence [3–7]. Предметом дослідження МР є різні види комп'ютерної інформації, що є результатом штатного функціонування ІТС. Основним методом її ведення є несанкціонований доступ (НСД) до такої інформації. Інструментами організації МР при цьому, як правило, виступають засоби знищення, перекручення чи розкрадання інформаційних масивів, засоби подолання систем захисту, засоби обмеження допуску законних користувачів до ресурсів ІТС, засоби дезорганізації роботи технічних засобів або комп'ютерних систем, комп'ютерні віруси, логічні бомби, засоби придушення інформаційного обміну в телекомунікаційних мережах, засоби нейтралізації тестових програм, а також різного роду помилки, що свідомо вводяться в ІТС [8].

Підкоряючись у цілому законам типового розвідувального циклу МР здійснюється шляхом моніторингу структури мережі, побудови її мапи, визначення точок уразливості мережі та мережевого трафіку. Разом з тим її суто специфічними етапами є [3]:

– вибір досліджуваної мережі (сервера) інформаційного простору;

– сканування, тестування, збір інформації про мережу (сервер);

– обробка даних, вибір уразливої точки для проникнення;

– використання уразливості з метою проникнення в систему.

Залежно від цілей діяльності, масштабу і характеру виконуваних завдань мережеву розвідку прийнято розділяти на стратегічну і тактичну. Для її організації і проведення нині використовують такі методологічні підходи, як, по-перше, перехоплення мережевого трафіка шляхом застосування мережевого сніфінгу, неправдивих запитів ARP, неправдивої маршрутизації або перехоплення TCP-з'єднання, по-друге, ідентифікація мережевих сервісів й, по-третє, сканування портів. За рахунок цього в ході проведення, наприклад, тактичної розвідки порушниками можуть бути виявлені дані щодо технічної і програмної оснащеності ІТС, уразливостей поштових серверів, сервісів і поштових клієнтів, меж сегментів мережі, використовуваних каналів зв'язку (тип, пропускна здатність тощо), приналежності мережі та/або сервера тощо, що у свою чергу, як результат, у подальшому вплине на

прийняття раціонального рішення із планування й проведення атак на ІТС (CITC). Інформація, що необхідна протиборчим сторонам під час проведення, наприклад, тактичної МР збирається з використанням великого набору загальнодоступних даних і додатків [3], головними серед яких є: формування запитів DNS (Domain Name System) [9], проведення ехо-тестування адрес (ping sweep), сканування портів [10, 11] тощо.

Результатом проведення активної і пасивної мережевої розвідки, що проводиться на тактичному рівні можуть бути дані, наведені у таблиці 1.

Таблиця 1

Результати проведення активної і пасивної мережевої розвідки, що проводиться на тактичному рівні

Результат активної МР	Результат пасивної МР
Доступні вузли на певному сегменті мережі. Розташування маршрутизаторів ті брандмауерів. Встановлені ОС на ключових вузлах. Відкриті порти. Працюючі сервіси та програмне забезпечення. Версії програмних продуктів, що використовуються.	Вузли, що є в одному сегменті з об'єктом розвідки. Встановлені ОС на ключових вузлах. Відкриті порти. Працюючі сервіси та програмне забезпечення. Дані про власника доменного імені, його адресу, адресу його електронної пошти, телефон. Географічне місце розташування об'єкта розвідки. Логін і пароль користувачів.

На рис. 1 наведена технологія організації і проведення мережевої розвідки з використанням уразливостей притаманних, наприклад, Web-ресурсам [3]. Для цього може бути використане як штатне ПЗ, представлене сканерами типу XSpider, Nessus, GFI LANguard Network Security Scanner, Microsoft Baseline Security Analyzer, Retina Network Security Scanner, Shadow Security Scanner, Shared resourse scanner та ним подібними, так і допоміжне – типу Cerberus Internet Scanner, Legion, Enum, Whatsrunning, Nmap, Netcat, Ethereal, Ettercap, VmWare тощо.

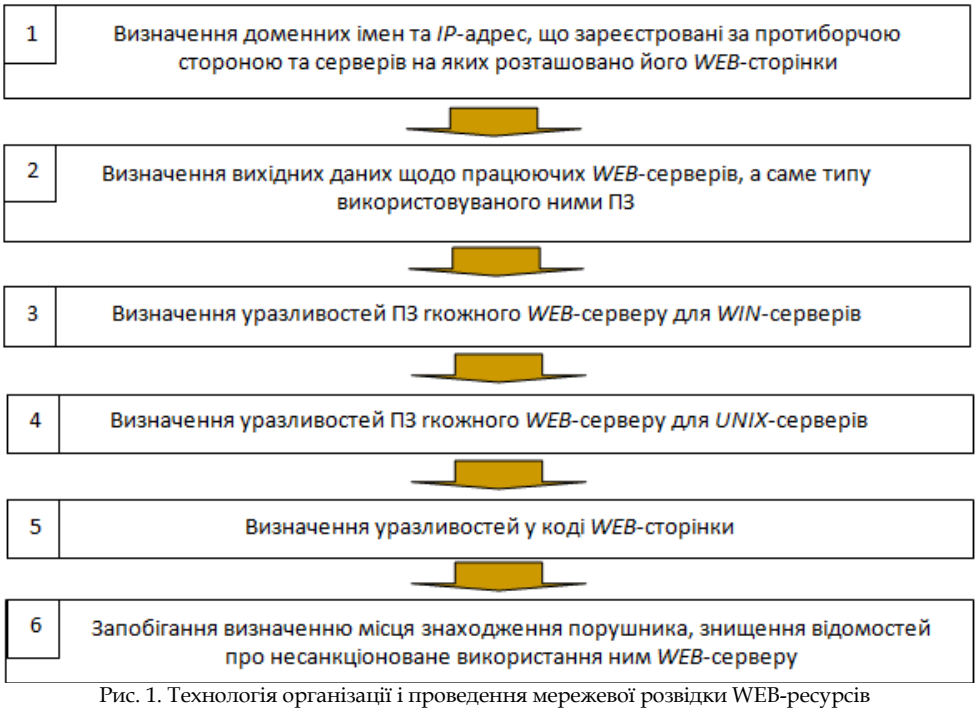

Рис. 1. Технологія організації і проведення мережевої розвідки WEB-ресурсів

При цьому першим кроком дій порушника має бути виявлення доменних імен та IP-адрес, що зареєстровані за об'єктом розвідки, а також серверів на яких розташовані його Web-сайти (сторінки). Такі дії здійснюються, як правило, шляхом:

– обрання об'єкта розвідки та вказівки його пошуковій системі. Результатом має стати отримання URL Web-сайтів (сторінок) об'єкта розвідки з яких можна визначити його доменне ім'я;

– введення на певних довідкових сайтах доменних імен (наприклад, таких як: www.dnsstuff.com, whois.com.ua, webnames.ru чи інших ним подібних) імені домену об'єкта розвідки. Результатом має стати визначення IP-адрес Web-серверів, на яких розташовані Web-сайти останнього.

На другому кроці шляхом сканування уразливостей ОС кіберпростору об'єкта розвідки за допомогою спеціалізованого ПЗ та надсилання завідомо некоректних запитів на доступ, проводиться уточнення даних про тип ПЗ працюючих Web-серверів. Результатом таких дій при, наприклад, неправильно заданій адресі документу (тобто, документу якого немає на сайті "www.someone.net/nevercreated.htm" або інших) може стати видача повідомлення про помилку 404 й, можливо, інформації про атрибути Web-серверу тощо.

На наступному, третьому кроці, здійснюються заходи з визначення уразливостей ПЗ Web-серверу для Win-серверів. Для цього шляхом сканування системи проводиться перевірка наявності в базах даних (знань) та бюлетенях безпеки на Web-сайтах www.bugtraq.ru, www.nessus.org, www.snort.org і Web-сторінках виробника, даних про вразливості Web-серверу. Пошук програм, що експлуатують знайдену вразливість, виконується на сайті http://www.securityfocus.com/ та інших. Залежно від кількості помилок, які притаманні даному сервісу, буде визначена відповідна кількість описів (можливо також з вихідними текстами програм, що експлуатують вразливість). При цьому вихідний текст програми, що експлуатує уразливість компілюється за допомогою ПЗ cc (на Windows системах): cc-s exploit.c-o exploit.exe. Визначення опцій запуску зазначеної програми здійснюється командою: D:\exploit.exe-h. Далі здійснюються спроби отримати привілеї адміністратора.

На четвертому кроці здійснюються заходи з визначення уразливостей ПЗ Web-серверу для Unix-серверів. Для цього шляхом сканування системи проводиться перевірка наявності в БД (БЗ) і бюлетенях безпеки на Web-сайтах www.bugtraq.ru, www.nessus.org, www.snort.org, а також Web-сторінках виробника даних про уразливості Unix-серверу. Пошук програм, що експлуатують знайдену вразливість, виконується на сайті http://www.securityfocus.com/. Залежно від кількості помилок, які притаманні даному сервісу, буде визначена відповідна кількість описів (можливо також з вихідними текстами програм, що експлуатують цю уразливість). При цьому вихідний текст програми, яка експлуатує виявлені уразливості компілюється за допомогою ПЗ gcc: gcc-s exploit.c-o exploit.exe. Визначення опцій запуску зазначеної програми здійснюється за командою D:\exploit.exe-h. У подальшому за допомогою скомпільованої програми та помилкових настроювань NFS здійснюються спроби отримати привілеї адміністратора та скачати з Unix-станції певну технологічну інформацію (файл з паролями). У разі використання Win-станції використовується ПЗ NFS: #showmount-e www.someone.net. За умови неотримання бажаного результату слід використати інше ПЗ.

На п'ятому кроці шляхом сканування системи, як це було зазначено вище та перевірки наявності в коді скриптів, що використовуються при роботі Web-сторінки (сайту), можливості проведення атак типу "PHP-including", "SQL-injection" або атак на CGI скрипти, – проводиться визначення відповідних уразливостей. При цьому в результаті виявлення, наприклад, в PHP коді можливості проведення атак типу PHP-including визначається параметр, якому передається посилання на ідентифікатор http://www.someone.net/ index. php?page=123. Після цього посилання змінюється на скрипт, який зберігається на створеній Web-сторінці, наприклад: http://www.someone.net/index.php?page =http://www.x. ru/x.php. Результатом таких дій є виконання стороннього скрипта на WEB-сервері, що може надати можливість здійснити неавторизований доступ до ресурсів Web-серверу.

При виявленні можливості проведення атак типу SQL-injection на Web-сторінки визначаються параметри, що передаються базі даних (знань). Таким чином можна отримати дані для несанкціонованого доступу до ресурсів Web-серверу, завдяки чому з'являється можливість у подальшому за допомогою отриманих даних передати SQL запит до БД із власними даними. Шляхом перебору таблиць, які створені в БД Web-серверу, визначається таблиця з даними про конкретних користувачів. Отримані дані можуть бути використані для отримання неавторизованого доступу до ресурсів Web-серверу. У разі виявлення недоліків у CGI-скриптах можна отримати доступ до системних файлів шляхом передачі відповідному параметру локальної адреси файлу, наприклад: http://www.someone.net/cgi-bin/staffs.cgi. При цьому параметру скрипта staffs.cgi file_name передається значення "../../../../etc/passwd", після чого скрипт повертає першу строку файлу. Також за допомогою подібних маніпуляцій можна закачати на сервер ПЗ типу webshell (cgitelnet.pl, j5.shell, cmd.cgi тощо) та отримати консольний доступ до ресурсів системи.

Шостий крок дій щодо організації та проведення атаки на Web-ресурси об'єкта розвідки полягає у виконанні порушником сукупності заходів із запобігання визначенню місця його знаходження, а також знищення відомостей про несанкціоноване використання ним Web-серверу. Для цього у Unix системі здійснюється збір інформації з певних журналів реєстрацій: #cat/etc/syslog.conf, а за рахунок ПЗ, використовуваного на третьому кроці, здійснюється переповнення буферу Web-серверу, як такого.

Висновки

Таким чином можна констатувати, що нині більшість країн світу й Україна, як суверенна та незалежна держава зокрема, зважаючи на відсутність розвиненої інформаційної та кіберінфраструктури, мають відносну захищеність національного інформаційного ресурсу та ринку інформаційних послуг від посягань на нього з боку будь-яких зацікавлених сторін. Одним з найбільш ефективних засобів профілактики, протидії та боротьби з найрізноманітнішими кібернетичними втручаннями і загрозами, поступово перетворюючись з діяльності щодо своєчасного викриття ознак підготовки імовірного противника до збройного нападу в діяльність, орієнтовану на досягнення та/або утримання над ним певної інформаційної переваги невдовзі стане розвідка ІТ систем.

Значне підвищення результативності розвідки ІТС у сучасних умовах може бути досягнуто шляхом активізації зусиль за напрямом РСТ, МР і КР. При цьому аналіз сучасних підходів та технологічних рішень щодо організації і проведення заходів, спрямованих на систематичний пошук, збір та/або добування даних про ресурси, засоби захисту,

пристрої та програмне забезпечення (ПЗ), що використовується в ІТС об'єкта розвідки, їх уразливі місця та межі проникнення дозволяє констатувати, що у перспективі найкращого результату слід очікувати саме від мережевої розвідки. Для цього передусім доцільно скомплектувати набір ПЗ для ефективного виконання заходів МР (на основі можливої модернізації відомих утиліт відкритого коду або розробки власних версій), забезпечити наявність деперсонофікованого підключення до зовнішньої Internet-мережі при відсутності дій Internet-провайдера з блокування та фіксування вищеозначених процедур розвідки, збільшити пропускну здатність каналів тощо.

Література

[1] Юдін О.К., Богуш В.М. Інформаційна безпека держави: Навчальний посібник. / О.К. Юдін, В.М. Богуш. – Харків: Консул, 2005. – 576 с.

[2] Ленков С.В. Методы и средства защиты информации. В 2-х томах / С.В. Ленков, Д.А. Перегудов, В.А. Хорошко; под ред. В.А. Хорошко. – К.: Арий, 2008. – Том I. Несанкционированное получение информации. – 464 с.

[3] Бурячок В.Л. Основи формування державної системи кібернетичної безпеки: Монографія. – К.:НАУ, 2013. – 432 с.

[4] Дудихин В.В. Конкурентная разведка в Интернет / В. В. Дудихин, О. В. Дудихина. – М.: АСТ, НТ Пресс, 2004. – 240 с.

[5] Ромачев Н.Р. Конкурентная разведка / Н. Р. Ромачев, И. Ю. Нежданов. – М.: Ось-89, 2007. – 272 с.

[6] Ющук Е. Конкурентная разведка. Маркетинг рисков и возможностей / Е. Ющук. – М.: Вершина, 2006. – 240 с.

[7] Павел П. Сетевая разведка. [Електронний ресурс] / П. Павел. – Режим доступу: http://www.warning.dp.ua/comp11.htm.

[8] Любарський С.В. Місце та роль мережевої розвідки в моделях інформаційного протиборства. / С. В. Любарський. Збірник наукових праць. Вип.. №1. – К.: ВІТІ НУТУ «КПІ», 2013. – С. 31–39.

[9] Карпов Г. Атака на DNS или ночной кошмар сетевого администратора. [Електронний ресурс] / Геннадий Карпов. – Режим доступу: http://www.hackzone.ru/articles/dns-poison.html, 02.06.2007.

[10] Разведка объектов атаки. [Електронний ресурс]. – Режим доступу: http://stfw.ru/page.php?id=11329.

[11] Examining port scan methods - Analyzing Audible Techniques. [Електронний ресурс]. – Режим доступу: http://www.windowsecurity.com/whitepapers/xamining_port_scan_methods_Analyzing_Audible_Techniques.html.

УДК 351.86:004.73.056 (045)

Бурячок В.Л. Технология использования уязвимостей web ресурсов в процессе организации и проведения сетевой разведки информационно-телекоммуникационніх систем

Аннотация. *Рассмотрено назначение и основные разновидности разведки информационно-телекоммуникационных систем (ИТС). Предложено определение разведки в системах телекоммуникации, сетевой (СР) и киберразведки. Определена сфера возможных интересов СР и методы ее ведения, а также место СР в общем процессе добывания информации. Рассмотрен пример использования уязвимостей Web ресурсов при организации и проведении СР ИТС.*

Ключевые слова: *информация, информационно-телекоммуникационная система, сетевая разведка.*

Buryachok V.L. Technology of using vulnerabilities of web resources in the process of organization & realization of network intelligence in information-telecommunication systems

Abstract. *The purpose and main types of the intelligence in information-telecommunication systems (ITS) were considered. A definition of intelligence in telecommunication systems, network (NI) & cyberintelligence were proposed. The scope of possible NI interest, its methods and also the place of NI in general process of information obtaining were defined. An example of using vulnerabilities of WEB resources in the process of organization & realization of NI in ITS was considered.*

Keywords: *information, information-telecommunication systems, network intelligence*

Отримано *30 квітня 2013 року*, затверджено редколегією 21 *травня 2013 року*