

Міністерство освіти і науки України
Київський університет імені Бориса Грінченка



ПРИКЛАДНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аналіз мережевого трафіку

Навчальний посібник



Львів
Видавництво «Магнолія 2006»
2024

*Рекомендовано до друку Вченою радою Київського університету імені Бориса Грінченка
(протокол №4 від 25.04.2019 р.)*

Автори:

Борсуковський Юрій Володимирович – кандидат технічних наук, Державний університет інформаційно-комунікаційних технологій;

Борсуковська Вікторія Юріївна – керівник проектів департаменту безпеки ПАТ «Укрсоцбанк»;

Бурячок Володимир Леонідович – доктор технічних наук, професор, Київський університет імені Бориса Грінченка;

Складанний Павло Миколайович – кандидат технічних наук, доцент, Київський університет імені Бориса Грінченка;

Гайдур Галина Іванівна – доктор технічних наук, професор, Державний університет інформаційно-комунікаційних технологій.

Рецензенти:

Самохвалов Ю. Я. – доктор технічних наук, професор;

Казмірчук С. В. – доктор технічних наук, доцент.

**Борсуковський Ю. В., Борсуковська В. Ю.,
Бурячок В. Л., Складанний П. М., Гайдур Г. І.**
Б 82 **Прикладні аспекти інформаційної та кібернетичної безпеки держави. Аналіз мережевого трафіку** : навч. посіб. / Борсуковський Ю. В., Борсуковська В. Ю., Бурячок В. Л., Складанний П. М., Гайдур Г. І. — Львів – Видавництво «Магнолія 2006», 2024. — 222 с.

ISBN 978-617-574-272-3

У підручнику розкриваються методологічні аспекти щодо дослідження поведінки мережевих додатків і вузлів з метою виявлення і виправлення проблем в роботі мережі для забезпечення інформаційної та кібернетичної безпеки підприємства. Нерідко, для вирішення таких проблем, спеціалісти з інформаційної та кібернетичної безпеки вдаються до використання аналізаторів мережевих пакетів.

Ключовими особливостями використання програмних аналізаторів пакетів є, по-перше, можливості різнобічної аналітики, а по-друге, багатофункціональна фільтрація пакетів, що дозволяє отримати витяги інформації, що потрібні нам для аналізу мережевого трафіку. Саме останньому аспекту і присвячений цей учбовий посібник.

Приводяться приклади практичного використання програмного аналізатора пакетів Wireshark для захвату і фільтрації мережевого трафіку. Розглядаються питання щодо вибору фільтрів для аналізу функціонування елементів мережі в найдрібніших деталях.

Підручник орієнтований на широке коло наукових та науково-педагогічних працівників, які займаються питаннями розроблення і застосування систем інформаційної та кібернетичної безпеки, а також фахівців, які працюють у галузях управління, планування та прогнозування ІТ, створюють перспективні або модернізують існуючі АС, ведуть дослідження за напрямками забезпечення безпеки та неперервності функціонування систем ІТ.

Викладений матеріал призначений для аспірантів та магістрантів вищих навчальних закладів, які навчаються за спеціальністю «Безпека інформаційно – комунікаційних систем» в галузі знань «Інформаційна безпека».

УДК 32.973я73 р.

ISBN 978-617-574-272-3

© Борсуковський Ю.В., Борсуковська В.Ю.,
Бурячок В. Л., Складанний П.М., Гайдур Г. І., 2024
© Київський університет ім. Б. Грінченка, 2024
© Видавництво «Магнолія», 2024

ЗМІСТ

ПЕРЕДМОВА	8
ТЕРМІНИ ТА ВИЗНАЧЕННЯ	10
Еталонна модель OSI.....	13
Ієрархічні івні моделі OSI	13
Прикладний рівень (Application Layer).....	16
Представлення рівень (Presentation Layer)	17
Сеансовий рівень (Session Layer).....	18
Транспортний рівень (Transport Layer)	18
Мережевий рівень (Network Layer).....	19
Канальний рівень (Data Link Layer).....	20
Фізичний рівень (Physical Layer)	21
Відповідність моделі OSI та інших моделей мережевої взаємодії	22
Протокол TCP/IP	23
Модель TCP/IP	25
Графічне пояснення моделей OSI і TCP/IP	28
Огляд програм для аналізу мережевого трафіку	31
SolarWinds Network Bandwidth Analyzer	32
WireShark	33
TCPdump	34
Kismet.....	35
EtherApe	36
Cain and Abel.....	37
NetworkMiner	37
KisMAC	38
Висновок.....	39
Введення в WireShark.....	40
Завантаження WireShark.....	40
Інструкції для роботи з WireShark	41
Інструкція користувача.....	42
Порівняння WireShark та його комерційних аналогів.....	42
Візуалізація проблем	44

Експертний аналіз на рівні додатків	45
Відновлення структури запитів	46
Тимчасова діаграма пакетів	48
Об'єднання потоків даних	49
Висновок	50
Використання WireShark	51
Встановлення і налаштування	52
Кольорове кодування	53
Захоплення пакетів	53
Навігація за списком	55
Управління стовпцями і їх вмістом	56
Упорядкування пакетів	56
Помилка «IP checksum offload»	58
Фільтрація пакетів	60
Фільтри захоплення пакетів	60
Фільтри відображення пакетів	61
Використання експертних опцій	72
Налаштування фільтрів для захоплення трафіку	73
Фільтр по протоколу	75
Фільтр по номеру порту	78
Фільтр по IP адресі і фільтр по MAC	80
Перелік типових фільтрів	83
Пошук конфліктуючих IP-адрес	84
Аналіз мережевого і транспортного рівнів	85
Аналіз HTTP-трафіку	87
Перехоплення SSL-контенту	89
Аналіз трафіку з віддалених хостів	90
Аналіз пакетів	91
Аналіз сеансів і TCP	92
Вилучення даних з трафіку	95
Вилучення VoIP трафіку	98
Сканування портів	100
Варіанти підключення до мережі для захоплення трафіку	101
Захоплення трафіку на стороні клієнта або сервера	101
Захоплення трафіку на комутаторі (SPAN)	103
Переваги SPAN сесії	105
Відгалужувачі мережевого трафіку (TAP)	106

Пошук складних непостійних проблем	111
Налаштування Wireshark для аналізу складних проблем	111
Налаштування «dumprcar» для захоплення пакетів	114
Особливості використання «dumprcar»	117
Аналіз SSL/TLS трафіку	123
Використання секретного ключа сервера	126
Використання секретів сесій	130
Розшифровка SSL/TLS трафіку через логування сесійних ключів браузера	132
Розшифровка TLS трафіку Java додатків	136
Розшифровка WPA2-PSK трафіку	144
Перехоплення паролів	150
Фільтрація захопленого POST трафіку	151
Логін і пароль користувача	151
Визначення типу кодування для розшифровки пароля	153
Розшифровка пароля користувача	153
Розшифровка HTTPS трафіку	153
Процес розриву з'єднання TCP Reset (TCP RST ACK)	155
Локалізація місця TCP Reset	156
Відправка TCP RST (SYN)	157
Відправка TCP RST (ACK)	157
TCP Retransmission	157
Ідентифікація повторних передач	159
Колонка «ACK to»	162
Моніторинг продуктивності сервера і мережі	163
Моніторинг користувача	164
Оцінка часу підключення користувача до сервера	164
Аналіз часу відгуку додатку	166
Локалізація причин	166
Висновки	166
Методика вирішення проблем з додатками	167
Аналіз продуктивності DNS-сервісу	169
Висновок	172
ДОДАТОК 1	174
Просте пояснення моделі OSI	174

ДОДАТОК 2	183
Перелік основних мережевих протоколів	183
ДОДАТОК 3	186
Телекомунікаційна мережа	186
Класифікація за географічним розташуванням	186
Класифікація за структурою взаємозв'язків (топологією)	187
Класифікація за режимом комунікації	188
Класифікація за швидкістю мережі	188
Принципи комунікації	188
Мережеві технології локальних мереж	189
Поняття фрейма	190
Комутація каналів	191
Комутація пакетів	191
Дейтаграма	192
Пакет даних	192
Механізм формування пакетів	192
Протокол визначення адрес (ARP)	193
Опис протоколу	193
ARP-таблиця для перетворення адрес	193
Порядок перетворення адрес	194
Запити та відповіді протоколу ARP	194
MAC-адреса	195
Адресація MAC-рівня	195
Мережа з комутацією каналів	196
Мережа з комутацією пакетів	196
Широкомовна мережа	197
ДОДАТОК 4	199
Поняття маршрутизатора	199
Принцип роботи маршрутизатора	199
Таблиця маршрутизації	200
Застосування	201
Перенаправлення портів і віртуальні сервери	201
Функції безпеки	202
Додаткові можливості	204

ДОДАТОК 5	206
ТСР-порти для SSL трафіку.....	206
Додаток 6	208
Перелік навчальних прикладів трафіку WireShark.....	208
ЗМІСТ	208
ДОДАТОК 6	212
Протокол Transport Layer Security (TLS)	212
Опис протоколу	212
Відкриття сеансу (рукостискання)	212
Алгоритми обміну/узгодження спільного ключа	214
Цифрові сертифікати	214
Відкликання сертифікатів	216
ЛІТЕРАТУРА	218

Навчальне видання

БОРСУКОВСЬКИЙ Юрій Володимирович

БОРСУКОВСЬКА Вікторія Юріївна

БУРЯЧОК Володимир Леонідович

СКЛАДАННИЙ Павло Миколайович

ГАЙДУР Галина Іванівна

ПРИКЛАДНІ АСПЕКТИ ІНФОРМАЦІЙНОЇ ТА КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ДЕРЖАВИ

Аналіз мережевого трафіку

Навчальний посібник

Підп. до друку 14.11.2023 р.

Формат 70x100/16. Папір друк. №2. Гарнітура PT Serif.

Умовн. друк. арк. 18,04.

Видавництво «Магнолія 2006»

м. Львів-53, 79053, Україна, тел.: +38 (050) 370-19-57

e-mail: magnol06@ukr.net

<https://magnolia.lviv.ua>

Свідоцтво про внесення суб'єкта видавничої справи до Державного реєстру видавців, виготівників і розповсюджувачів видавничої продукції: серія ДК № 2534 від 21.06.2006 року, видане Державним комітетом інформаційної політики, телебачення та радіомовлення України

Надруковано у друкарні видавця Марченко Т. В.