THE USE OF PACKET SNIFFING TOOLS IN COMPUTER NETWORKS SECURITY

Damna S. Ahmedova, Ekaterina M. Konstantinova, Tsvetoslav S. Tsankov

[1] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Student, dsezginova@gmail.com
[2] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Student, katminkova2@gmail.com
[3] Faculty of Technical Sciences at Konstantin Preslavsky – University of Shumen, Bulgaria, Assoc. prof. Eng., PhD, c.cankov@shu.bg

***Abstract**: With each passing year, computer networks are evolving, increasing the number of devices involved in network traffic. The extremely large number of packages hides a large number of dangers, which calls for specialized detection software. The publication features Wireshark, which is a typical representative of Packet sniffing software.*

***Keywords**: Network security, Networking sniffing, Packet analyzer, Packet capture, Wireshark*

ИЗПОЛЗВАНЕТО НА ИНСТРУМЕНТИ ЗА ПРОСЛУШВАНЕ НА ПАКЕТИ ЗА БЕЗОПАСНОСТ НА КОМПЮТЪРНИТЕ МРЕЖИ

Дамна С. Ахмедова, Екатерина М. Константинова, Цветослав С. Цанков

Въведение

В компютърните мрежи всеки ден могат да се проявяват милиони най-разнообразни случаи – от проста зараза с шпионски софтуер, до сложни грешки в конфигурацията на рутера. От полза за всички е осигуряването на информация и предпазни техники за справяне със злонамерените събития.

Особено важно за работата по затрудненията при компютърните мрежи е опитните аналитици да работят на ниво пакети. Точно на това ниво започват всички затруднения, могат да се наблюдават лоши реализации дори и на най-добре изглеждащите приложения и протоколите да се окажат зловредни. Нищо на това ниво не е скрито, не се наблюдават привлекателни графики, заблуждаващи менюта, няма секретна информация, освен специално шифрираната.

Именно поради това може най-добре да се контролира мрежата на ниво пакети и своевременно да се разрешават проблемите чрез анализиране на пакети [1], [4].

Подслушването в мрежата може да се използва за улавяне на идентификационни данни, съобщения в чата и дори прехващане на файлове, предавани по мрежата. Процесът на подслушване се използва от хакерите за директно прехващане на данни, или за да добият представа за детайли по мрежата, които ще им помогнат за бъдеща атака.

Анализиране на пакетите

Анализирането на пакетите или протоколите трябва да описва процеса на прехващане и интерпретиране на данните според движението им по мрежата, за да може по-добре да се узнае какво се случва. По правило анализирането на пакетите се извършва от анализаторите на пакети, които представляват инструменти за прехващане на първични данни, предавани по преносната среда.

Анализът на пакетите може да е полезен за следното:

- да се пояснят характеристиките на мрежата;
- да се изяснят намиращите се в мрежата;
- да се определи кой или какво „изяжда“ пропускателната способност на мрежата;
- да се изяснят моментите, когато използването на мрежата достига своя връх;
- да се изяви зловредната дейност в мрежата;
- да се открият опасните и големите приложения.

За анализиране на пакетите са предлагани различни програми – безплатни и платени. Всяка от тези програми има своята цел, а най-разпространените са `tcpdump` в команден ред и OrnniPeek и Wireshark, които имат графичен потребителски интерфейс [6], [7].

При избора на програма за анализиране на пакетите, под внимание трябва да бъдат взети редица фактори:

— поддръжка на мрежовите протоколи – всички анализатори на пакети поддържат различни протоколи, като например най-разпространените мрежови протоколи (IPv4 и ICMP), транспортните протоколи (TCP и UDP) и протоколи на приложно ниво (DNS и HTTP). Това са главните протоколи, а по-сложните (т.напр., IPv6, SMBv2 и SIP) могат да не се поддържат от анализаторите на пакети;

— удобство за използване – от особена важност е интерфейса на програмите, лесната работа с анализатора на пакети и точната последователност на операциите. Програмата да съответства на квалификацията на този, който я използва, като например `tcpdump` никак няма да е подходяща за начинаещи, а за опитните са необходими дори и по-сложни програми;

— стойност – това за някои е най-важното условие, но не и при анализаторите на пакети, т.к. повечето от тях са безплатни и с нищо не са по-лоши от платените. Разбира се заплатените имат едно важно предимство – модул за оформяне на отчети, които са доста по-скромни при безплатните анализатори;

— програмата да има поддръжка – тя ще е от особено значение, когато възникват нови задачи и трябва да се обърнем към общности, работещи с програмата и събираща бази от знания за всякакви ситуации;

— достъп до изходния код на програмата – по-напредналите използват програми с отворен код, за да могат да внасят корекции и за да услужат на собствените си изисквания;

— поддръжка на операционна система – не са много програмите, които са достъпни за всякакви операционни системи, но това е проблем с малка тежест, т.к. не е трудно специалиста да научи друг анализатор на пакети за работа с друга операционна система.

При анализирането на пакети освен софтуер се използва и хардуер, като процеса се дели на три етапа:

1. *Събиране на данни*. Анализаторите на пакети събират първични данни от мрежите в двоичен вид. Това става с превключване на избрания мрежов интерфейс в смесен режим (promiscuous mode), при който мрежовата карта може да приема целия трафик, а не само адресируемия до нея.

2. *Преобразуване*. Първичните двоични данни трябва да се преобразуват в четима форма, т.напр. при анализаторите с команден ред, при които обаче мрежовите данни се интерпретират на най-елементарно ниво, а анализа остава задача на потребителя.

3. *Анализ*. Последната работа на анализаторите на пакети е да проведат анализ на прехванатите и преобразувани данни. Това става чрез проверка на протокола за прехванатите данни и извличане на характерните особености на този протокол [2], [5], [8].

Анализаторът Wireshark

Програмата Wireshark е създадена през 2006 г. като наследник на програмата Ethereal от 1998 г. Тя има редица предимства според изискванията посочени по-горе:

— Wireshark поддържа всички мрежови протоколи, които са около 1000, като при всяко обновление се прибавят и още;

— програмата е с един от най-опростените графични интерфейси, контекстни менюта и много други удобства дори за начинаещи потребители;

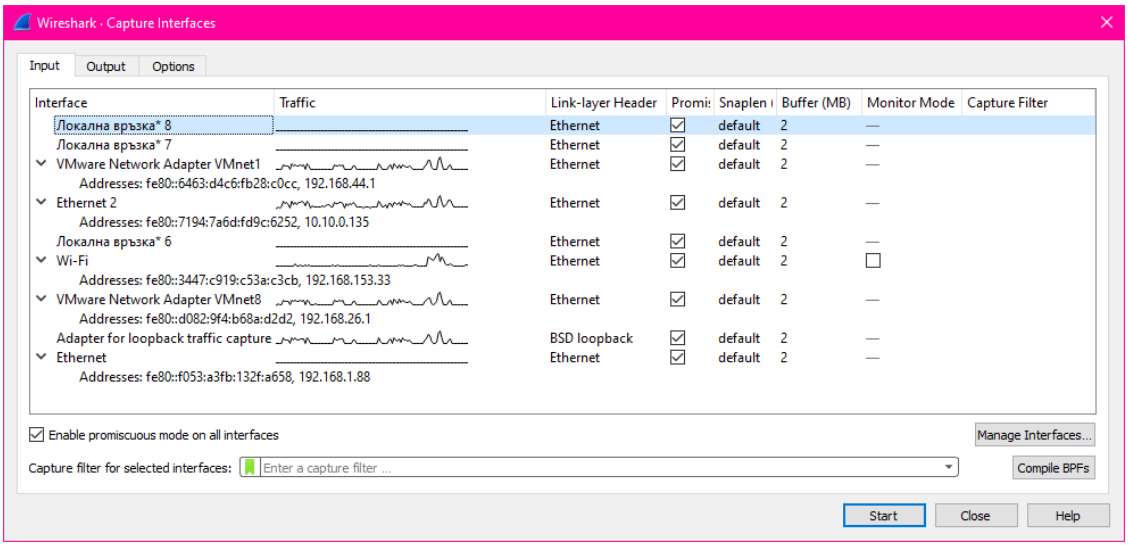
— Wireshark се разпространява безплатно;

— съобществото на поддръжниците, оказващи помощ за разработчиците на Wireshark, се състои от най-активните членове;

— всеки напреднал потребител може да персонализира кода, поради принадлежността на програмата към софтуер с отворен код;

— още едно огромно предимство е, че приложението е достъпно за всички основни съвременни операционни системи, като например Windows, Linux и Mac OS X.

Първото нещо, което трябва да се направи е да се избере мрежов адаптер (фиг. 1). Това става от меню Capture – Options.

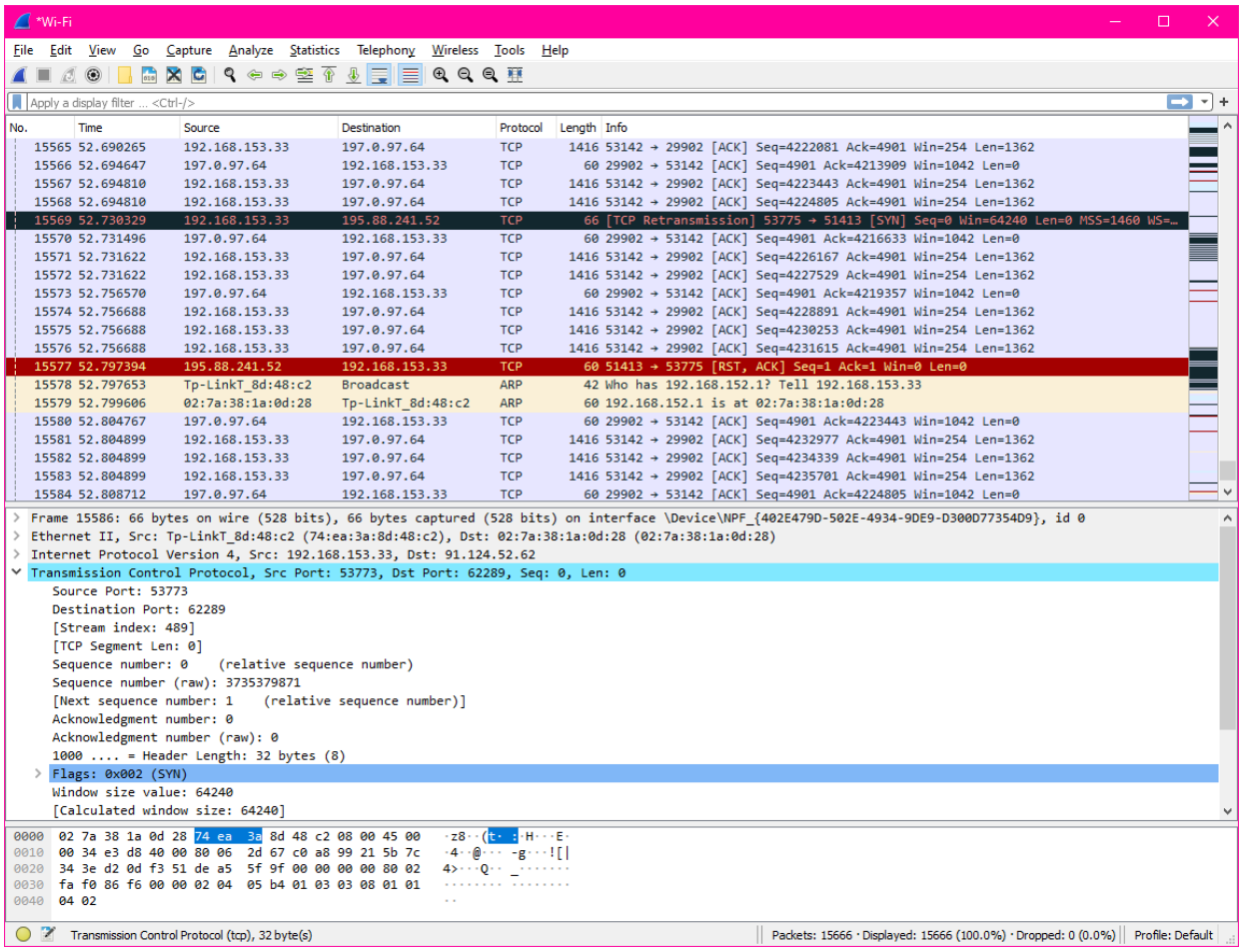


Фиг. 1: Избор на мрежов интерфейс

В появилия се диалогов прозорец са изредени всички мрежови интерфейси, които са достъпни за прехващане на пакети, заедно със съответните сведения за тях. В колонката Traffic

излизат линейните графики на активен трафик в реално време за всеки интерфейс, като пиковите точки указват прехващане на пакети.

След стартирането за прехващане на данни от избрания интерфейс, трябва да се изчака и да се спре изпълнението. Отчетените данни вече запълват главния прозорец на Wireshark, където те са в удобен за анализиране формат (фиг. 2).



Фиг. 2: Главен прозорец на Wireshark

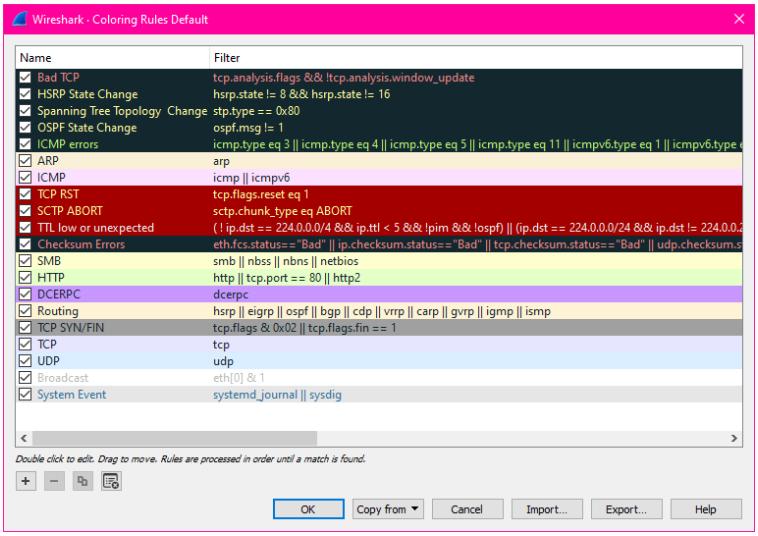
В главния прозорец на Wireshark са панелите Packet List (списък на пакетите), Packet Details (подробни сведения за пакети) и Packet Bytes (байтове на пакети). От Packet List се избира даден пакет, за който излизат подробни сведения в Packet Details, където ако се избере част от пакета, то в панела Packet Bytes ще се появят съответните байтове на тази част. Вижда се потока от пакети с подробна информация [3], [9].

Списъкът с пакети показва всякакви мрежови протоколи от различни нива, като се различават единствено по различното оцветяване. Всички пакети са в такъв ред, в какъвто са получени. Тази таблица показва всички пакети от текущото прехващане. В колонките са номер на пакета, относително време на прехващането, IP адрес на източника, IP адрес на получателя, протокол използван за предаването и някои общи сведения.

Подробните сведения за пакети е панел, който показва в йерархичен вид сведения за един пакет. Може да се свива и разгъва за показване на цялата информация, която е събрана за даден пакет.

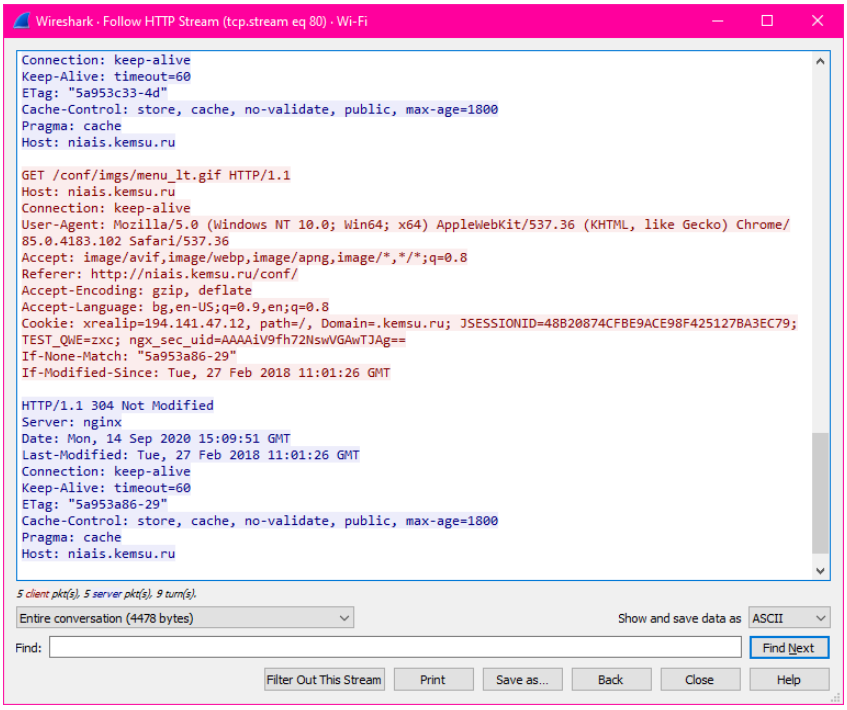
Байтовете на пакетите показват изходните данни на пакета в необработен вид – такъв, какъвто го пренасят по мрежата [6], [9].

Wireshark видно разграничава трафика според протоколите. Това става удобно с помощта на цветово кодиране с различни цветове. Това оцветяване може да бъде персонализирано (фиг. 3).



Фиг. 3: Цветни кодове на Wireshark

Една от най-полезните функции за анализиране на сесии е Stream Capture (прехващане на потоци), удобна за протоколи като HTTP, SMTP и FTP (фиг. 4).



Фиг. 4: HTTP Stream Capture

Заключение

Софтуерът за анализиране на пакети е от основните инструменти на мрежовия администратор и на разследващите киберпрестъпления. Използването на подслушването може сериозно да навреди, т.к. може да улавя потребителски имена и пароли, както и друга чувствителна информация. Тези инструменти правят добро в ръцете на добрите и лошо в ръцете

на злодеятелите. Подслушването и анализирането на пакети трябва да направи компютърните мрежи с по-добра производителност и с повишена безопасност [1, 7, 8].

References

1. Bhandari, A., Gautam, S., Koirala, T.K., Islam, M.R. (2018). *Packet Sniffing and Network Traffic Analysis Using TCP-A New Approach*. Advances in Electronics Communication and Computing, Springer, ISBN 978-981-10-4764-0.
2. Boyanov, P., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Educational simulation the local area network of academic departments with securely configured FTP server*. International Scientific Online Journal, www.sociobrains.com, Publ.: Smart Ideas - Wise Decisions Ltd, ISSN 2367-5721 (online), Issue 31, March 2017, Bulgaria, pp. 146-154.
3. Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Routing information security in the local area network of academic departments using an enhanced distance vector routing protocol – EIGRP*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 35-46.
4. Boyanov, P., Stoyanov, St., Hristov, Hr., Fetfov, O., Trifonov, T. (2017). *Security routing simulation the local area network of academic departments using a link-state routing protocol – OSPF*. A refereed Journal Scientific and Applied Research (Licensed in EBSCO, USA), Konstantin Preslavsky University Press, ISSN 1314-6289, vol. 11, pp. 47-58.
5. Kazakov, S., Yankova-Yordanova, Y. (2017). Typology of risks in RFID. Journal Scientific & Applied Research, Vol. 12, ISSN 1314-6289.
6. Sanders, C. (2017). *Practical packet analysis*. No Starch Press, ISBN 978-1-59327-802-1, San Francisco.
7. Saxena, P., Sharma, S.K. (2017). *Analysis of Network Traffic by using Packet Sniffing Tool: Wireshark*. International journal of advance research, ideas and innovations in technology, Vol. 3, Issue 6, ISSN 2454-132X.
8. Siswanto, A., Syukur, A., Kadir, E.A., Suratin (2019). *Network Traffic Monitoring and Analysis Using Packet Sniffer*. 2019 International Conference on Advanced Communication Technologies and Networking (CommNet), Rabat, Morocco, ISBN 978-1-5386-8317-0.
9. Wireshark User's Guide. Version 3.3.0.