

Учреждение образования
«БЕЛОРУССКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ИНФОРМАТИКИ И РАДИОЭЛЕКТРОНИКИ»

Кафедра интеллектуальных информационных технологий

Отчет по лабораторной работе №3
по курсу «СиМОИБ»
на тему: «Наблюдение за стеком TCP/IP»

Выполнил студент группы 421702:

Бруцкий Д.С.

Проверил:

Захаров В.В.

Задание для самостоятельной работы

- Установите программы, необходимые для перехвата сетевого трафика.
- Изучите различные параметры работы программ для перехвата сетевого трафика.
- Выполните анализ трафика (с различными параметрами детализации):
 - ping запроса,
 - HTTP трафика при загрузке любого веб-ресурса,
 - аутентификацию в веб-ресурсе, на котором не настроен HTTPS,
 - SSH, SCP трафика,
 - FTP трафика и т. д.
- Определите, к каким портам и адресам были выполнены обращения.
- Используя дополнительную литературу, расшифруйте содержание перехваченных пакетов.

Ход работы:

Для перехвата и анализа сетевого трафика использовалась программа network monitor

Ping запрос:

При вызове команды ping она отправляет ICMP пакет по указанному адресу и дожидается ответа, затем отправляет еще 3 раза.

117862	22:39:04 04.12.2016	2336.0574492	RIZHI-KOTE	95.213.11.144	ICMP
117863	22:39:04 04.12.2016	2336.1193169	95.213.11.144	RIZHI-KOTE	ICMP
117864	22:39:05 04.12.2016	2337.0611629	RIZHI-KOTE	95.213.11.144	ICMP
117865	22:39:05 04.12.2016	2337.0923897	95.213.11.144	RIZHI-KOTE	ICMP
117866	22:39:06 04.12.2016	2338.0638712	RIZHI-KOTE	95.213.11.144	ICMP
117867	22:39:06 04.12.2016	2338.0969874	95.213.11.144	RIZHI-KOTE	ICMP

Аутентификация в веб-ресурсе, на котором не настроен HTTPS.

При аутентификации на сайте без HTTPS можно из перехваченного пакета достать логин пароль, переданные на сайт. Были перехвачены пакеты с сайта rutracker.org . На снимке ниже приведен перехваченный пакет, содержащий передаваемую информацию пользователя.

113311	23:15:57 04.12.2016	1482.6910177	firefox.exe	RIZHI-KOTE	RUTRACKER.ru	HTTP	HTTP:Request, POST /login.php
113532	23:15:58 04.12.2016	1484.3055249	firefox.exe	RUTRACKER.ru	RIZHI-KOTE	HTTP	HTTP:Response, HTTP/1.1, Status:
113542	23:15:58 04.12.2016	1484.3350548	firefox.exe	RUTRACKER.ru	RIZHI-KOTE	HTTP	HTTP:HTTP Payload, URL: /login.php
113619	23:15:59 04.12.2016	1484.4900262	firefox.exe	RIZHI-KOTE	185.49.146.51	HTTP	HTTP:Request, GET /v1/code.js, Qu

Frame Details		Hex Details
Upgrade-Insecure-Requests: 1 ContentType: application/x-www-form-urlencoded ContentLength: 98 HeaderEnd: CRLF payload: HttpContentType = application/x-www-form-urlencoded redirect: %2F login_username: Dimqn login_password: Devil autologin: on login: %D0%92%D1%85%D0%BE%D0%B4		Decode As Width 000A FF 00 00 00 0014 00 00 00 00 001E D2 01 08 01 0028 CF C0 80 56 0032 27 D6 CF C0 003C 00 00 08 00 0046 40 00 80 06 0050 C1 69 F0 5E 005A E8 8E F5 C6 0064 7E AB 00 00

Анализ FTP трафика.

Number	Time Date Local Adjusted	Time Offset	Process Name	Source	Destination	Protoc...	Description	Conv Id
0	23:46:49 04.12.2016	1173.0217212	chrome.exe	RIZHI-KOTE	lyusin.MCCME.ru	FTP	FTP:Request from Port 57459, 'SYST'	(TCP:1183, IPv4:216)
1	23:46:49 04.12.2016	1173.1318146	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '215 UNIX Type: L8'	(TCP:1183, IPv4:216)
2	23:46:49 04.12.2016	1173.1320054	chrome.exe	RIZHI-KOTE	lyusin.MCCME.ru	FTP	FTP:Request from Port 57459, 'PWD'	(TCP:1183, IPv4:216)
3	23:46:49 04.12.2016	1173.1755931	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '257 "/" is the current directory'	(TCP:1183, IPv4:216)
4	23:46:49 04.12.2016	1173.1757415	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Request from Port 57459, 'TYPE I'	(TCP:1183, IPv4:216)
5	23:46:49 04.12.2016	1173.2117456	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '200 Type set to I'	(TCP:1183, IPv4:216)
6	23:46:49 04.12.2016	1173.2118953	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Request from Port 57459, 'SIZE /pub/video/cat.avi'	(TCP:1183, IPv4:216)
7	23:46:49 04.12.2016	1173.2534756	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '213 12414168'	(TCP:1183, IPv4:216)
8	23:46:49 04.12.2016	1173.2536133	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Request from Port 57459, 'CWD /pub/video/cat.avi'	(TCP:1183, IPv4:216)
9	23:46:49 04.12.2016	1173.3552268	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '550 /pub/video/cat.avi: No such file or directory'	(TCP:1183, IPv4:216)
10	23:46:49 04.12.2016	1173.3553722	chrome.exe	RIZHI-KOTE	lyusin.MCCME.ru	FTP	FTP:Request from Port 57459, 'PASV'	(TCP:1183, IPv4:216)
11	23:46:49 04.12.2016	1173.4225599	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '227 Entering Passive Mode (195,178,216,3,140...'	(TCP:1183, IPv4:216)
12	23:46:49 04.12.2016	1173.4617967	chrome.exe	RIZHI-KOTE	lyusin.MCCME.ru	FTP	FTP:Request from Port 57459, 'RETR /pub/video/cat.avi'	(TCP:1183, IPv4:216)
13	23:46:49 04.12.2016	1173.5180280	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '150 Opening BINARY mode data connection for ...'	(TCP:1183, IPv4:216)
14	23:47:27 04.12.2016	1211.1255517	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '451 Transfer aborted. Broken pipe'	(TCP:1183, IPv4:216)
15	23:47:27 04.12.2016	1211.3757512	chrome.exe	lyusin.MCCME.ru	RIZHI-KOTE	FTP	FTP:Response to Port 57459, '451 Transfer aborted. Broken pipe'	(TCP:1219, IPv4:216)

Frame Details		Hex Details
Ipv4: Src = 195.178.216.3, Dest = 192.168.0.100, Next Protocol = TCP, Packet ID = 204C Tcp: [Segment Lost]Flags=...AP..F, SrcPort=FTP control (21), DstPort=57459, PayloadLen= Ftp: Response to Port 57459, '451 Transfer aborted. Broken pipe' ReplyCode: 451, Requested action aborted. Local error in processing ReplyMessage: Transfer aborted. Broken pipe		Decode As Width Prot Off: 3 (0x03) Frame Off: 107 (0x6B) 003C 00 00 08 00 45 20 00 4B 4F B7 ... E . KO 0046 00 00 37 06 D7 13 C3 B2 D8 03 ... 7 . Å . Ø 0050 C0 A8 00 64 00 15 E0 73 27 C1 Å . d . Å s ' Å 005A C6 6A F6 65 67 3C 50 19 01 00 Æ j ö e g < P . . 0064 98 7C 00 00 34 35 31 20 54 72 . . 4 5 1 T 006E 61 6F 73 66 65 72 20 61 62 6F transfer abo

Вывод:

В данной работе я наблюдал за сетевым трафиком проходящим через сетевую карту. А именно за стеком протоколов TCP/IP. Исследовав пакеты протоколов UDP, TCP, FTP замечено что все они используют протокол IP на сетевом уровне. В ходе проведения работы было замечено, что наблюдать за чужим трафиком очень просто. У большинства протоколов не предусмотрено никакой аутентификации, у FTP есть возможность аутентифицировать пользователя с помощью пароля, но передача этих данных ничем не защищена.