УДК 004.728.4.056.53

ПЕРЕХВАТ ПАРОЛЕЙ В ОТКРЫТЫХ WI-FI СЕТЯХ С ПОМОЩЬЮ ПРОГРАММЫ INTERCEPTER-NG

Ерошевич К. В, студент гр. ИТб-132, 4 курс Научный руководитель: Алексеева Г.А., ст. преподаватель Кузбасский государственный технический университет имени Т.Ф. Горбачева г. Кемерово

В наше время широко распространены открытые точки доступа Wi-Fi. Но мало кто задумывается о сохранности своих персональных данных подключаясь к открытой точке Wi-Fi.

Подключившись к открытой точке Wi-Fi, можно обеспечить доступ к своим персональным данным третьим лицам, не поняв этого.

В качестве примера будет рассмотрена программа Intercepter-NG. Данная программа позволяет не только перехватывать пароли от сайтов, но и заменять сайты и многое другое.

После запуска программы, нужно выбрать сеть в графе «Network Adapter», к которой подключен компьютер (рисунок 1).



Рисунок 1

Следующим шагом производим настройку программы. Окно настройки представлено на рисунке 2.

Sniffer Configuration	MiTM Configuration
🗹 Resolve Hosts 🔲 Autosave	Spoof IP\MAC IP Forward
🔲 Lock on Tray 🗹 Grid View	🗹 iOS Killer 🗹 Cookie Killer
🔲 Save Session 🔲 eXtreme Mode	Kerberos Downgrade
🗹 Promiscuous 🔲 Capture Only	HSTS Spoofing 0
🗹 Unique Data 🛛 🗹 Resurrection	
IM Ports	Remote Capture (RPCAP)
5190,9898,5222,5050,1863,8074,	rpcap://192.168.1.1 not host 192.1 🗖 On
HTTP	PCAP Over IP (PORT)
80,3128,8080,1080,61111,61112,	2002 🗖 On
SOCKS	WPAD Configuration (PR0XY:P0RT)
1080,61111	📃 🔲 Built-in Proxy
6665,6666,6667,6668,6669,7000,	
	• • •

Рисунок 2

Следует отметить следующие опции:

- Resurrection для перехвата Cookie HTTPS;
- Cookie Killer, чтобы заставить пользователя снова вводить пароль.

После проведенных манипуляций необходимо запустить программу.

Далее нужно выбрать в меню пункт «MiTM Mode» и в «MiTM Option» следует нажать на изображение, отмеченное на рисунке 3 цифрой 2.

83	
Gateway	Statistics [IN]: UDP: 0 TCP: 0 [0UT]: UDP: 0 TCP: 0 [MiTM]: IN: 0 OUT
Stealth	MiTM Options
Third-Party SMB Server	🖉 🚟 🐼 🖉
Target	

Рисунок 3

В открывшемся окне (рисунок 4) нужно отметить «SSL MiTM» и «SSL Stip».

MiTM Attacks

SSL MITM	DNS<>ICMP	🔲 SMB Hijack	🗌 GP Hijack
🔽 SSL Strip	WPAD MITM	SSH MITM	
	O	<	
	Рисун	юк 4	

Выполним еще пару действий и программой можно пользоваться. Перейдем в соответствующую вкладку и выберем пункт «Smart Scan». Появятся все устройства, подключенные к сети Wi-Fi. Выбираем объект и в контекстном меню пункт «Add as Target» (рисунок 5).

IP	MAC		Vendor
<mark>=</mark> 192.168.1.60	DE-AD-DE	CENE AN	
👌 192.168.1.59	00-0	Set as Gatev	way
👌 192.168.1.1	38-2	Add as Targ	jet -
		Set as Stealt	th
		Resolve	
		Isolate from	n Gateway
		X-Scan	



Далее перейти на вкладку с изображением ключей. В этой вкладке будут отображаться логины и пароли, введённые объектом перехвата на сайтах.

В качестве примера рассмотрим на сколько защищены сайты <u>aist.kuzstu.ru</u> (HTTP протокол), <u>portal.kuzstu.ru</u> (HTTPS протокол).

1. Сектор содействия трудоустройству выпускников <u>aist.kuzstu.ru</u>

Введенные данные л	огин: User; пароль: password (рисунок 6). ▼3G∡ G∡ ■ 85 % 21:33
	aist.kuzstu.ru/index.php/vh 1
	Е СЕКТОР СОДЕЙСТВИЯ ТРУДОУСТРОЙСТВУ ВЫПУСКНИКОВ
	Логин * User 3 а Пароль * Д а
	войти в о п
	Забыли пароль?
	Забыли логин?
	Ещё нет учётной записи?

Рисунок 6

Результат работы программы представлен на рисунке 7.

-	-	<u> </u>	<u> </u>	÷ •	
Protocol	Time/Date	From/To	Host	Username	Password
HTTP Auth	21:34:54	192.168.1.59/193	aist.kuzstu.ru/index	username=User	&password=password

Рисунок 7

2. Портал КузГТУ portal.kuzstu.ru

Введенные данные логин: User; пароль: password (рисунок 8).

https://portal.kuzstu.ru	1	:
\bigcirc		
Вам необходимо авторизоваться для запрашиваемой странице	до <mark>ступа</mark> к	
Логин		
User		
Пароль	_	
Войти		
Забыли пароль?		
Сайт КузГТУ		
Разделы системы, доступные без авто	ризации:	

Рисунок 8

D	~				0
Pegymt TgT n	200TLI TO	OFDAMMET	πηρηγηρηρι	ua nucuuve	x
		UI Dammidi	представлен	πα υπό γπκο	· O.
					-

		eersi mperper	продотив	ion ne projine	<u>.</u>
Protocol	Time/Date	From/To	Host	Username	Password
HTTP Auth	21:34:54	192.168.1.59/193	aist.kuzstu.ru/index	username=User	&password=password
Web Site visited	21:38:32	192.168.1.217/19	192.168.1.217	portal.kuzstu.ru	
HTTPS Auth	21:38:51	192.168.1.217/19	portal.kuzstu.ru/auth	username=User	&password=password

Рисунок 8

Как видно программа работает даже в случае использования HTTPS протокола.

Из всего выше сказанного можно сделать следующий вывод перехватить персональные данных легко, а «подарить» их еще легче, даже если Вы пользуетесь сайтами по HTTPS протоколу. Поэтому прежде чем воспользоваться открытыми Wi-Fi точками доступа, следует очень хорошо подумать, так ка неизвестно кто и для каких целей может ими пользоваться вместе с Вами.

Список литературы:

1. Intercepter-ng.com[Электронный ресурс] URL: <u>https://intercepter-ng.com</u>