?????????? ??????????

Снижение активности в сети

Этот принцип — один из самых простых с точки зрения технического исполнения, но в то же время является сложным из-за необходимости проявить креативность. Наша максимальная задача в этом процессе — не оставить возможности детектирования наших действий активными средствами защиты.

Шаги для снижения активности в сети:

- Исключить все возможные типы сканирования портов, так как этот процесс достаточно легко детектируется даже через сканирование портов на одном узле.
- Перед обращением к какому-либо узлу сети продумывать, не попадем ли мы в HoneyPot, и почему выбранный нами узел — точно не HoneyPot.
- Исключить совершение атак типа “Man in The Middle”.

Какие подходы могут помочь нам исследовать сеть и определиться в пути компрометации:

- Обращаться только к тем сервисам, с которыми работают пользователи в сети.
- Исследовать DNS имена в трафике и в домене, пытаясь обнаружить наиболее интересные машины в сети.
- Исследовать ARP запросы в сети, для того чтобы пассивно собирать информацию об участниках сети.
- Обращаться к общедоступным ресурсам в домене.
- При сканировании сервисов использовать подключение только к отдельным портам без флагов активного сканирования.

Примеры приемов по снижению активности в сети

1. Опросить DNS на предмет корневых доменных имен.

> dig domain.local

2. Опросить домен на предмет записей о сервисах в домене.

> dig -t SRV _gc._tcp.domain.local
> dig -t SRV _ldap._tcp.domain.local
> dig -t SRV _kerberos._tcp.domain.local
> dig -t SRV _kpasswd._tcp.domain.local

3. Исследовать трафик сети на предмет широковещательного трафика: ARP, mDNS, LLMNR, NBTNS и пр.

4. Попытаться обратиться к общедоступным ресурсам, типа почты, сервера LDAP, сервера, WPAD прокси.

> dig -t MX domain.local

> dig -t wpad.domain.local

Использование шифрованных каналов связи

Для того, чтобы активные средства защиты не могли обнаружить атакующий трафик и определить опасные конструкции в нем по сигнатурам, необходимо постоянно заботиться о том, чтобы наш трафик эксплойтов или команд невозможно было расшифровать.

Если наша задача — применить эксплойт, то желательно работать только с применением шифрования трафика прикладных протоколов (например, используя SSL/TLS).

Это могут быть такие протоколы, как:

- HTTPS
- SMB (только версии 3.1.1 и выше)
- SMTP (только на порте 465 с использованием команды STARTTLS)
- SSH

Также критически важно использовать шифрованные каналы связи с взаимодействием с нагрузкой для контроля и выполнения команд. Для этого в фреймворке C&C необходимо использовать нагрузки с связью по каналам, использующим TLS. Например, в metasploit:

```
windows/meterpreter/reverse_https (В LHOST необходимо будет указывать доменное имя)
windows/meterpreter/reverse_winhttps
windows/meterpreter_reverse_https (нагрузка без стейджера)
```

Revision #1
Created 13 October 2025 08:43:24 by Admin
Updated 13 October 2025 08:47:33 by Admin